APPENDIX L

Installation Information Infrastructure Architecture (I3A) Implementation Guide

DEPARTMENT OF THE ARMY

UNITED STATES ARMY INFORMATION
SYSTEMS ENGINEERING COMMAND
FORT HUACHUCA, ARIZONA 85613-5300

TECHNICAL GUIDE FOR INSTALLATION INFORMATION INFRASTRUCTURE ARCHITECTURE

BY
FREDERICK M. SKROBAN II

INTERIM
AUGUST 2003

FORT DETRICK ENGINEERING OFFICE

Distribution C
Distribution authorized to U.S. Government agencies and their specified contractors only, for administrative or operational use, August 2003. Refer other requests for this document to Commander, U.S. Army Information Systems Engineering Command, ATTN: AMSEL-IE-DE, Fort Detrick, MD.

DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for advertisement.

CHANGES

Refer requests for all changes that affect this document to USAISEC, ISED, ATTN: AMSEL-IE-IS, Mr. Ronald Corry, Building 53301, Arizona Street, Fort Huachuca, AZ 85613-5300; DSN 879-3173 or commercial (520-) 538-3173; corryr@hqisec.army.mil

DISPOSITION INSTRUCTIONS

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.

TECHNICAL GUIDE
FOR
INSTALLATION INFORMATION
INFRASTRUCTURE ARCHITECTURE

BY

FREDERICK M. SKROBAN II

AUGUST 2003

INTERIM

U.S. ARMY INFORMATION SYSTEMS ENGINEERING COMMAND

FORT DETRICK ENGINEERING OFFICE

Distribution C

Distribution authorized to U.S. Government agencies and their specified contractors only, for administrative or operational use, August 2003. Refer other requests for this document to Commander, U.S. Army Information Systems Engineering Command, ATTN: AMSEL-IE-DE, Fort Detrick, MD.

Product Certification

Signatures on file in the S&IG indicate the Director's approval of the Technical Guide content and the CSE/CSH certification that the Guide format meets the requirements of the Letter of Instruction for Preparation of Technical Guides, AMSEL-IE-TD, 14 June 2002.

Approval Dates:

CSE/CSH: ______

Director: ________

Signature, Technical Director: _____________________

TABLE OF CONTENTS

LIST OF DRAWINGS

TABLE OF CONTENTS (CONTINUED)

TECHNICAL GUIDE FOR INSTALLATION INFORMATION INFRASTRUCTURE ARCHITECTURE

1.0 INTRODUCTION

1.1 Purpose

This document provides guidance for the planning, design, and implementation of the Installation Information Infrastructure Architecture (I3A) for Army installations in the Continental United States (CONUS). This document will establish an implementation concept that can be used to shape architectural templates and influence the design process for the I3A. It will identify proven infrastructure construction techniques, define common practices, and serve as an authoritative implementation guide.

1.2 Background

In previous engineering designs each area of communications was addressed separately, to include design standards, schedule, and funding. This approach led to confusion, design re-engineering, and duplication of effort. The I3A concept was initiated to synchronize the efforts and formulate a more efficient and effective design process. I3A establishes an Army-wide Information Technology (IT) architectural design standard. I3A is the source to fuel effective Army Knowledge Management necessary to support the Army Transformation Campaign Plan. I3A captures installation infrastructure, synchronizes the implementation of automation programs, provides for analysis of operational force and sustaining base connectivity, and identifies costs associated with IT modernization. The I3A Configuration Control Board (CCB) manages I3A issues and tracks developments in IT, information assurance, enterprise systems management and automation information systems (AIS). The CCB, which oversees several working groups that address IT issues, meets quarterly.

1.3 Goal

This document will assist the communications designer by supplying common standards and architecture. Through the use of this document, all communications engineering should follow the same standards that will facilitate a concerted installation effort.

1.4 Scope

This document is intended to support the necessary requirements gathering, site surveys, analysis, design and implementation of Information Technology. This guide also assists the designer in the integration of the premise wiring, Local Area Network (LAN), Outside Plant (OSP) cabling, network backbone, voice switching, network management and information security.

1.5 I3A Program Synchronization

Integration of architectures throughout the Army and Department of Defense (DoD) is essential. The I3A is a synchronization tool for major Army automation and communications programs (Figure 1-1: I3A Program Synchronization). Under the major Army automation programs such as Defense Communications and Army Switched System, this guide also assists in the integration of the Outside Cable Rehabilitation (OSCAR), Common User Installation Transport Network (CUITN), Army Defense Information Systems Network (DISN) Router Program (ADRP), Installation Information Infrastructure Modernization Program (I3MP), and Digital Switched Systems Modernization Program (DSSMP), The underlying objective is to meet current information transfer requirements while creating an infrastructure sufficiently flexible to meet the exponentially increasing future data communications requirements and to accommodate new technology advances. A long-term benefit of the I3A is to accommodate the transmission of voice, video, and data.

1.5.1 I3A Technical Review Process

The major objective of the I3A Synchronization and Technical Review Process is to assist in implementation and maintenance of a MACOM/DOIM installation infrastructure. Specific objectives are the elimination of "drive-by fielding" and the facilitation of local and MACOM infrastructure initiatives. To accomplish these objectives the MACOM, DOIM, or PM should submit an Infrastructure Upgrade Plan to the U.S. Army Information Systems Engineering Command (USAISEC) prior to implementing network changes. The POC for USAISEC is Mr. Craig Engel, DSN 879-3172/Commercial (520) 538-3172, e-mail address: engelc@hqisec.army.mil

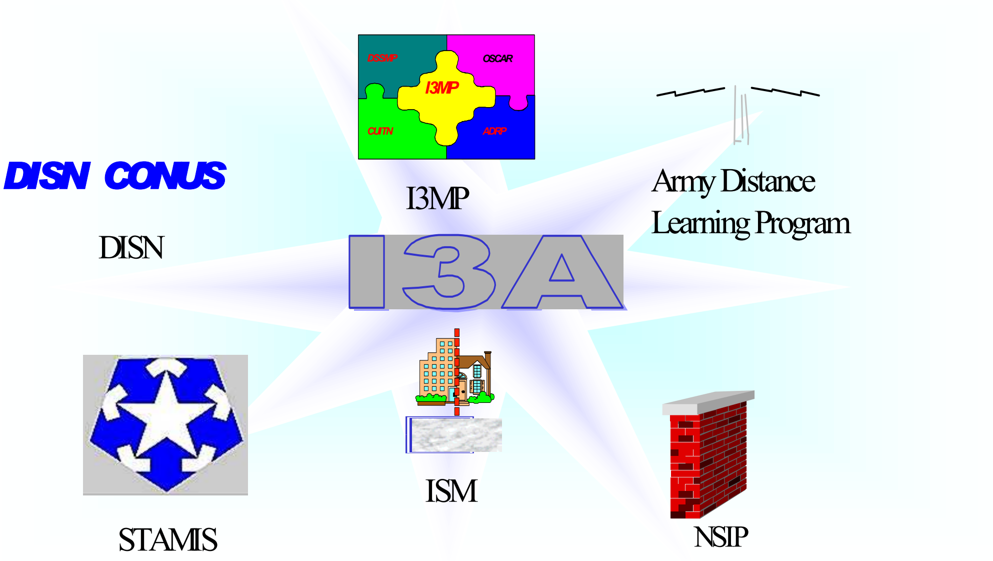


Figure 1-1: I3A Program Synchronization

1.5.1.1 Infrastructure Upgrade Plans

The IUPs should address the following areas:

- All outside connections, including DISA Non-secure Internet Protocol Routing Network (NIPRNET), Secure Internet Protocol Router Network (SIPRNET), dial-up connections or any other network links.
- Top Level Architecture (TLA) equipment, to include security router, Intrusion Detection System (IDS), any and all Demilitarized Zones (DMZ), and Firewalls.
- Network System Management/Enterprise System Management (NSM/ESM) monitoring equipment and tools used
- **Army DISN Router Program (ADRP) Router**
- Main Communication Node (MCN) equipment (or equivalent)

- Area Distribution Node (ADN) equipment (or equivalent)
- Backbone cabling (to include type of cabling, i.e. SM FO, plus number of strands)
- EUB Edge Device equipment

1.5.2 Technical Guidance

Applicable policies and programs should be reviewed prior to infrastructure or network planning. This review ensures integration with current systems and enables the designer to identify programs and standards that provide procedural or technical guidance at the outset of the project. Planning includes identifying technologies and selecting the templates and topologies that best fit installation requirements.

1.5.3 Department of Defense Architectural Standards

The DoD has established a broad body of information technology standards, architecture, and design guidance. This guidance is incorporated in a hierarchy of standards and architectural guidance documentation that is available on the world wide web (www). These standards include the Joint Technical Architecture (JTA) (http://www-jta.itsi.disa.mil/) and JTA-Army (JTA-A) (http://arch-odisc4.army.mil/).

1.5.3.1 DoD Directives (DoDD) and DoD Instructions (DoDI)

In addition to the above hierarchy of architectural standards, DoD has created and implemented detailed guidance regarding interoperability among Command, Control, Communications, and Intelligence (C^3I) systems, and their supporting systems. This I3A Implementation Guide is in compliance with all these Interoperability Policy Documents.

1.5.4 Integrated Transfer System

The Army's goal of a common, fully integrated, digital transfer system is expected in the 2010+ time frame. For providing this service, Layer 3 switching using Gigabit Ethernet (GbE) is expected to support the communications infrastructure. The I3A infrastructure will support multimedia (voice, data, image, and video) communications. The I3A program will provide an infrastructure capable of supporting the integration of the voice telephone network and computer data networks. I3A is applicable to the design and engineering of new buildings and other projects under the Army military construction programs, as well as in the installation, rehabilitation, and replacement of current installation telecommunications infrastructure. The following figure reflects an example of an integrated network.

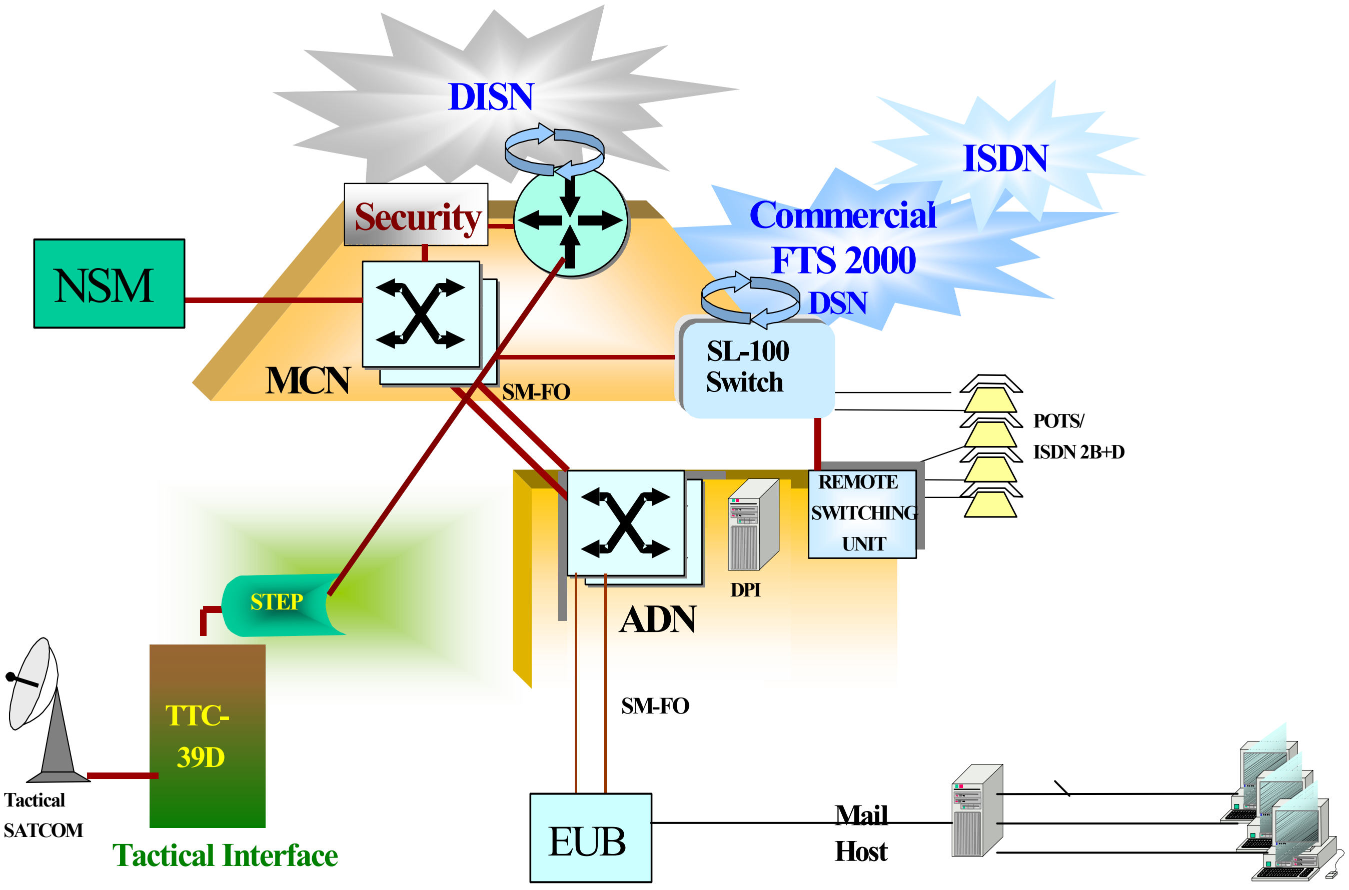


Figure 1-2: I3A Integrated Layout

Note: The I3A should be capable of connecting the tactical and sustaining base in support of the Army Warfighter as a key component of the Force Projection concept. However, tactical interfaces are currently not included this document.

1.6 Document Content

This document is composed as follows:

- Section One – Introduction
- Section Two – Premise Distribution System
- Section Three – Outside Plant
- Section Four – Dial Central Office/Remote Switching Unit
- Section Five – Network Architecture
- Section Six – Network and Systems Management
- Section Seven – Network Security
- Section Eight – Acronyms

- Section Nine – Legend of I3A symbols

1.7 Future Concerns and Planning

The system designers must consider the future user requirements that will impact the network, i.e. projected growth, higher processing speeds and throughput.

1.7.1 Advanced Applications

More advanced user requirements and bandwidth sensitive applications (e.g., tele-medicine, desktop video teleconferencing, and educational applications) require faster processors and distributed client/server computing that are driving the enterprise network evolution to upgrade the information infrastructure. All require higher performance/throughput, greater network predictability, higher network availability, and enhanced security than is currently available in the existing communications infrastructure.

1.7.2 Challenges

Installation networking engineers and designers face challenges such as systems integration, interoperability, identifying the most efficient technologies, and leveraging government contracts for purchasing equipment. This document assists the planner in making informed decisions that are technically correct and financially feasible.

1.7.3 Future Growth

The advent and spread of services such as Video Teleconferencing (VTC), Voice over IP (VoIP), streaming video, and the migration towards web based documentation has led to a desire for larger bandwidth and faster connection. At the same time, most users are currently connected to an ISDN capable switch for voice and a LAN for data. The designers for Information Infrastructure should look at the future needs, and ensure that new designs meet not only the immediate needs, but also leave room for growth. The designed supporting infrastructure should allow the migration to higher data transfer rates and more data intensive services.

1.8 Outside CONUS Implementation

The engineer or designer of Outside CONUS (OCONUS) projects should consider the requirements and practices of the signal command responsible for the OCONUS location in question. Some of the regional signal commands have policies that cover I3A in the specific host nation or area. The Engineer should also consider the agreements with, or policies of the host nation for use of products, personnel, and architecture, prior to implementing a design. This guide provides solutions that follow the guidance of primarily North American standards agencies and committees. This guide can be used as a normative reference, but the designer should consider the standards in use at the specific location as stated above.

2.0 PREMISES DISTRIBUTION SYSTEM

2.1 Premises Distribution System Specifications

The Premises Distribution System (PDS) is designed to satisfy I3A policy information system (IS) requirements within a facility. The PDS should be installed in accordance with the Telecommunications Industry Association (TIA) and Electronics Industry Association (EIA) Building Telecommunications Wiring Standards general guidelines with modifications and clarifications provided below. TIA/EIA specifications can be purchased at http://www.tiaonline.org/standards/. Please note that the specifications, physical plant, and inside plant components discussed below reflect objective architectural concepts that may or may not need to be adapted.

2.2 ANSI/TIA/EIA Standards

ANSI/TIA/EIA-568-B.1 Commercial Building Telecommunications Cabling Standard, Part 1: General Requirements

ANSI/TIA/EIA-568-B.2 Commercial Building Telecommunications Cabling Standard, Part 2: Balanced Twisted Pair Cabling Components

ANSI/TIA/EIA-568-B.3 Commercial Building Telecommunications Cabling Standard, Part 3: Optical Fiber Cabling Components

ANSI/TIA/EIA-569-A Commercial Building Standard For Telecommunications Pathways and Spaces

ANSI/TIA/EIA-526-7 Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant

ANSI/TIA/EIA-526-14A Measurement of Optical Power Loss of Installed Multimode Fiber Cable Plant

ANSI/TIA/EIA-606 Administrative Standard for the Telecommunications Infrastructure of Commercial Buildings

ANSI/TIA/EIA-607 Commercial Building Grounding and Bonding Requirements for Telecommunications

2.2.1 Classified Information Infrastructure

Engineers engaged in the design of classified (collateral or higher) Information Infrastructure shall coordinate the infrastructure design with the Certified TEMPEST Technical Authority and accrediting organization responsible for that area. This Technical Guide cannot attempt to replace the publications that have been produced to support the design of Red/Black infrastructure. The Engineer shall consult the following applicable documents for consideration and design guidance: NSTISSAM TEMPEST/2-95 (FOUO) defines the guidance to consider during design and installation, and provides potential solutions, DCID 1/21 (U) defines the physical security requirements in construction of secure facilities, NSTISSP 300 (U) provides the National Policy on the Control of Compromising Emanations, and NSTISSI 7003 (U) provides guidance on Protected Distribution Systems. Additional information on grounding can be found in MIL-STD-188-124B and MIL-HNBK-419-A.

2.3 Workstation Outlet

The following specifications pertain to telecommunications and connector outlets:

2.3.1 Outlet Box

For standard administrative and medical facility (hospital) outlets use a recess mounted 4-11/16" by 4-11/16" double gang electrical box with the faceplate flush with the wall surface. Double gang electrical boxes should be full depth to provide dedicated space for current and possible future fiber optic cable installation. For single connector outlets, such as voice, data, cable television (CATV) or closed circuit television (CCTV), use a full depth, single gang, electrical box recess mounted, with the faceplate flush with the wall surface.

2.3.2 Outlet Faceplate

For standard administrative outlets use a full (double gang) faceplate with connector locations for all copper and (if used) fiber optic cable. Standard administrative outlets may, by specific user request, use single gang outlet faceplates in conjunction with a reducing ring. For single gang outlet boxes, use a single gang outlet faceplate with appropriate connector locations and, if required, mounting lugs for wall phones.

2.3.3 Outlet Connectors

The following specifications pertain to copper, fiber optic and coaxial cable connectors.

2.3.3.1 Copper Connectors

Copper connectors should be EIA/TIA category 6 (Cat 6) or enhanced category 5 (Cat 5e), 8-pin/8-position insulation displacement terminations wired per T568A (default configuration) or T568B (if required to maintain system configuration uniformity, security or other user-specified reasons). Category 3 (Cat 3) rated connectors should not be used in new construction or rehabilitation projects. Copper connectors and plugs should be unkeyed unless the user requires keyed connectors and plugs to maintain system uniformity, security, or other user specified reasons.

2.3.3.2 Fiber Optic Connectors

The default choice for fiber optic connectors should be EIA/TIA "SC" type (568SC). EIA/TIA "SC" type connectors are preferred in new systems as the international standard now accepted by the Federal Government. Small form factor connectors (available from several manufacturers), offer a potential for significant installation cost reduction, however the EIA/TIA has declined to select any individual product for inclusion in the standards. Any type of fiber connector used shall meet the performance requirements specified within Annex A of TIA/EIA-568-B.3, and meet the requirements of the corresponding TIA Fiber Optic Connector Intermateability Standard (FOCIS) document.

2.3.3.3 Coaxial Connectors

Coaxial connectors should normally be “F” type connectors. Use of other type connectors (i.e., BNC, etc.) should be considered only if specifically required by the user. The designer should coordinate with the cable service provider where franchise agreements are in place.

2.3.4 Outlet/Connector Markings

Each communications outlet should have a unique identifying number. In the telecommunications room (TR), this unique identifying number should be associated with the position on the patch panel or cross connect to which the outlet is connected. Each horizontal cable should be labeled both at the outlet and patch panel or cross-connect position in the communications closet.

2.3.5 Outlet Types

The following outlet types are commonly used in military construction projects. Sketches of these outlets are included in Figure 2-5: Telecommunications Outlet Types.

a. Administrative Outlet. Two 8-pin modular (RJ45 type) connectors in a single or double gang outlet faceplate, one connector dedicated to voice use and one dedicated to data use.

b. Administrative w/Fiber Outlet. Two 8-pin modular (RJ45 type) connectors in a single or double gang outlet faceplate, one connector dedicated to voice use and one dedicated to data use, and two fiber optic connectors, dedicated to data use. Use of administrative outlets with fiber optic connectors is at specific user request for each project.

c. Medical Facility (hospital) Outlet. Two 8-pin modular (RJ45 type) connectors in a double gang outlet faceplate, one unkeyed, dedicated to voice use, one keyed or unkeyed, dedicated to data use, and two dedicated blank positions for fiber optic connectors. Use of keyed modular connectors for data and installation of fiber optic connectors is at specific user request for each project.

d. Furniture Outlet. Two 8-pin modular (RJ45 type) connectors in a modular furniture outlet faceplate with outlet box extender, one connector dedicated to voice use, and one connector dedicated to data use. Connector voice and data dedication may be reassigned as requirements dictate. Use of modular furniture outlets with fiber optic connectors is at specific user request for each project.

e. Wall Outlet. One 8-pin modular (RJ45 type) connector in a single gang outlet faceplate with mounting lugs dedicated to voice use.

f. Special Outlet (FAX, Counter Top, etc.). Configuration generally similar to administrative or wall outlets but dedicated to special use and mounted at special heights usually defined by user (i.e., wall outlet mounted at 18’’ (450mm) above finished floor, or administrative outlet mounted just above countertop level.)

g. Pay Phone Outlet. One 8-pin modular (RJ45 type) connector in a single gang outlet faceplate with mounting lugs dedicated to voice use.

h. Barracks Outlet. One 8-pin modular (RJ45 type) connector in a single gang outlet faceplate, dedicated to voice use.

i. Barracks Outlet (TRADOC Schools). Two 8-pin modular (RJ45 type) connectors in a single gang outlet faceplate, one dedicated to voice use and one dedicated to data use.

j. Barracks Outlet (Combination). One 8-pin modular (RJ45 type) connector in a single gang outlet faceplate, dedicated to voice use, and one "F" type connector, dedicated to CATV or CCTV use.

k. Coaxial Cable Outlet. One "F" type connector, dedicated to CATV, CCTV or other video or data use.

l. User Defined Outlet. Number and type of connectors as defined by user.

2.3.6 Outlet Density

For planning purposes, when actual outlet locations are not known and cannot be determined with available information, reasonably accurate total outlet count estimations can be obtained based on the size and dedicated usage of the space. Calculations are based on gross square footage (overall building footprint without deducting for hallways, equipment rooms, restrooms, etc.), and the average outlet density for that specific category of facility space. See Figure 2-8: Typical Floor Plan for a typical building floor plan. Currently, ten categories of facility space are identified, each with its own average outlet density. The factors fall within the ranges given in TIA/EIA-569-A.

	Facility Space Category	Area (SF) per Outlet
a.	Administrative Space	80
b.	Laboratory/Technical Space	100
c.	Barracks Space	315
d.	Medical/Clinic Space	80
e.	Classroom XXI Space	80
f.	Warehouse Space	5000
g.	General Instruction/Other SPACE	500
h.	Clerical	140
i.	High Density	50
j.	Army Family Housing Units	see below

For Army Family Housing (AFH) Units, the number of rooms in the AFH unit determines minimum outlet quantities. In general provide one telephone outlet and one CATV outlet (as a minimum) in each of the following rooms: kitchen, living room, dining room, family room/area, each bedroom, and any other logical location deemed appropriate.

2.3.7 Utility Rooms and Closets.

All utility rooms and closets, such as electrical, mechanical and telecommunications, should be wired with at least one wall mounted telecommunications outlet, with a mounting lug face plate . House Wiring

The following information pertains to horizontal cable and vertical cable risers.

2.3.8 Horizontal Cable

The following information pertains to fiber optic cable and cable run lengths.

2.3.8.1 Copper Voice and Data.

Two Cat 6, 4-pair 24 American Wire Gauge (AWG), 100-ohm, solid, unshielded twisted pair (UTP) cables should be installed to each standard dual connector outlet and one Cat 6, 4-pair 24 AWG, 100 ohm, solid, UTP cable should be installed to each single connector outlet. Use only cable that has passed the Underwriters Laboratory (UL) LAN certification program and is labeled with UL acceptable markings. Plenum cables should be specified when required. Termination should be performed using an 8-pin (RJ45 type) connector. All terminations should be wired in accordance with TIA/EIA T568A. In a standard cabling scheme, horizontal cables are arbitrarily designated "voice" and "data" to identify and differentiate their purpose. Each voice outlet should be assigned a unique telephone number.

2.3.8.2 Fiber Optic Data

Fiber optic cable to each outlet is optional at specific user request. As a minimum, administrative (including hospital) outlet boxes and faceplates should be sized and configured to allow for the future installation of two strands of fiber optic cable. When the user requires fiber optic cable, 50/125-micron or 62.5/125-micron multi-mode cable should be installed using duplex "SC" type connectors. Single-mode fiber optic cable and other type connectors may be substituted as required by the user. Any type of fiber connector used shall meet the performance requirements specified within Annex A of TIA/EIA-568-B.3, and meet the requirements of the corresponding TIA Fiber Optic Connector Intermateability Standard (FOCIS) document. Plenum cables should be specified when required. Plenum cables should be specified when required.

2.3.9 Cable Length

Copper data cable length should be limited to 295 feet from patch panel termination in the TC to the data outlet termination in accordance with EIA/TIA-568-B.1. For planning purposes, in most administrative buildings where the TC is centrally located, assume an average of 120 feet of cable from the TC to each outlet. For non-administrative buildings (example: barracks), building renovations, or where the TC is not centrally located, adjust the average cable length for planning purposes as required (i.e., average measured length).

2.3.10 Vertical Riser Cable

The following subparagraphs pertain to copper and fiber optic cable.

2.3.10.1 Copper

Multi-pair voice riser cable should meet the requirements of Insulated Cable Engineers Association (ICEA) S-80-576 and EIA/TIA-568-B.2 for Cat 5 100-Ohm unshielded twisted pair cable. Conductors should be solid un-tinned copper, 24 AWG. The voice riser cable originating in the main TC or main cross connect should be terminated in each TC on 110 type punch blocks mounted on the telephone backboard. Provide at least two riser cable pairs for every outlet connected to the TC served by the riser cable. Plenum cables should be specified when required. ICEA specifications are listed, and can be purchased at http://global.ihs.com.

2.3.10.2 Fiber Optic

A minimum of 12 strands of 50/125-micron or 62.5/125-micron multimode fiber optic cable and 12 strands single mode fiber optic cable should be installed between the main telecommunications room or main cross connect and each TC. The data fiber optic cable riser should be terminated in a patch panel installed in an equipment rack or cabinet. If requested by the user, only 12 strands of one type of fiber may be used. Any type of fiber connector used shall meet the performance requirements specified within Annex A of TIA/EIA-568-B.3, and meet the requirements of the corresponding TIA Fiber Optic Connector Intermateability Standard (FOCIS) document. Plenum cables should be specified when required. The designer should note that the network architecture recommends single mode fiber optic cable between TCs. Plenum cables should be specified when required.

2.3.11 Coaxial Cable.

When CATV or CCTV requirements are identified, either a 75-ohm broadband coaxial cable or single-mode fiber optic cable system should be installed. When a coaxial system is installed, care should be taken to ensure the correct cable is used. The designer should coordinate with the cable service provider where franchised agreements are in place. Plenum cables should be specified when required. The table below lists cable type with corresponding distance limitation. This table is derived from vendor specifications (Anixter) for coaxial cable.

Cable	Distance
RG-59	<=150 feet
RG-6	<=250 feet
RG-11	<=400 feet

2.3.12 Building Infrastructure.

See Figure 2-1-A: Telecommunications Room Entrance and Riser and Figure 2-1-B: Telecommunications Room Horizontal Distribution for details.

2.3.12.1 Cable Tray.

Solid bottom cable tray should be used to provide a centralized cable management/distribution system. See Figure 2-2: Telecommunications Room Standard Premise Distribution for details. Provide a cable tray with one square-inch of cross-sectional area per outlet location to be served. [(For 30 outlets, a 9” by 4” (36 square-inches) cable tray would be satisfactory.] During actual design, an optimal fill ratio of 40% should be accommodated., Under no circumstances should the fill ratio exceed 60%. Ladder cable tray should be avoided.

2.3.12.2 Enclosed Duct (Raceway).

When a building design does not provide for installation of cable tray, enclosed square duct may be installed. Enclosed duct may also be used in place of cable tray when cable plant requires physical security. For initial design guidance, provide 1 square inch of cross-sectional area of the enclosed duct per outlet location. During actual design, an optimal fill ratio of 40% should be planned for, under no circumstances should a fill ratio of 60% be exceeded.

2.3.12.3 Conduit.

Electrical metallic tubing (EMT) conduit should be installed from the cable backbone distribution system, whether cable tray or enclosed duct, to each outlet. Conduit for standard outlets should be a minimum of 1-inch EMT conduit. When cable tray or enclosed duct is not used, individual conduits should be installed from the TC to each outlet. Where fiber optic cable is not initially installed to the standard dual connector outlets, a pull line should be installed in each conduit. An optimal conduit fill ratio of 40% should be accommodated., Under no circumstances should a fill ratio of 60% be exceeded.

2.3.12.4 Pull Cord.

All empty conduits routed to outlet boxes should be provided with a pull cord. All 1-inch conduits containing only copper communications cabling routed to administrative and hospital outlet boxes shall be provided with a pull cord for future installation of fiber optic cable.

2.3.12.5 Pull Boxes.

Pull boxes should be placed in conduit runs where a continuous conduit length exceeds 100 feet, or where there are more than two 90-degree bends. Pull boxes should be placed in straight runs of conduit and not be used in lieu of a bend.

2.3.12.6 Systems Furniture Wiring

The use of interconnected systems furniture has become more prevalent in the current office environment, and presents some unique challenges for the communications designers and implementers. Although systems furniture is designed for quick reconfiguration of office space, experience has shown that power and communications connections within the system furniture cannot be reconfigured easily.

2.3.5.6.1 Direct Connection.

Figure 2-6: Systems Furniture Wiring shows two possible solutions for direct wiring to the systems furniture. This concept is one of a continuous home run from the TC to the furniture outlet. Continuous runs allow flexibility in cabling. Testing of the installed cable plant is simplified by providing an end-to-end circuit, without an additional connection point.

2.3.5.6.2 MultiUser Telecommunication Outlet Assembly (MUTOA)

TIA/EIA-568-B.1 section 6.4.1 allows for MUTOA within an open office. This option provides greater flexibility in an office that is frequently reconfigured, but does introduce an additional connection and point of loss. If the MUTOA is used, it should be sized to support the number of users in the area plus 25%.

2.3.5.6.3 Consolidation Point (CP)

The consolidation point (CP) in TIA/EIA-568-B.1 section 6.4.2 provides a different interconnection point in the horizontal run. A CP cannot be used in conjunction with a MUTOA. The CP is an additional connection in the cable run.

2.3.5.6.42.3.5.6.3 Protection and Separation.

The implementers should ensure the cable is protected at all transition points, and that metallic separation is provided between telecommunication and power wiring in the power pole and/or systems furniture track.

2.3.12.7 Optional PDS Items

In new construction, particularly in large administrative or medical facility buildings, cable distribution systems should use the cable tray (or duct) and conduit systems as described. In new construction involving small, mixed use (non administrative) facilities, or construction projects involving renovation of existing buildings, use of “J” hooks, flexible cable tray, and alternative support systems specifically certified for Cat 6 cable is permissible. Polyvinyl chloride (PVC) surface mounted duct should be used in renovation projects where access to the walls for installation of conduit and outlet boxes is not possible, or where historical requirements prohibit the alteration of the building structure. See Figure 2-7: Premise Distribution Supporting Structure - Renovations for details.

2.4 Telecommunications Closet/Room.

See Figure 2-2: Telecommunications Room Standard Premise Distribution, , and Figure 2-4: for sample closet layouts. TIA/EIA-568-B.1 has replaced telecommunications closet (TC) with telecommunications room (TR). TIA/EIA-569-A has not yet been updated to reflect this change. The engineer should use the reference to telecommunications room to more accurately describe the space needed for telecommunications equipment.

2.4.1 Multi-Story Buildings.

In multi-story buildings, a minimum of one TR should be located on each floor (small facilities, i.e., air traffic control towers, firing ranges, etc., may use one TR for the entire facility). TRs on successive floors should be vertically stacked wherever possible. A minimum of three 4-inch rigid steel conduits should be installed between stacked closets on successive floors, in accordance with EIA/TIA 569A.

2.4.2 Closet Sizing.

TRs should be sized in accordance with EIA/TIA-569-A for all new construction projects with primarily administrative function (small mixed-use facilities should not require full compliance with EIA/TIA-569-A). Generally, the TR should be sized to approximately 1.1% of the area it serves. For example, a 10,000 square foot area should be served by a minimum of one 110-square foot TR. TR sizing allowances should be made only in cases of construction projects involving building renovation, and under no circumstances should a closet be smaller than 70 square feet (7’ x 10’).

2.4.3 Closet Interior Finishes.

Floors, walls, and ceilings should be treated to eliminate dust. Finishes should be light in color to enhance room lighting.

2.4.4 Closet Door.

TR doors should be a minimum of 36” wide, 80” tall, hinged to open outward (or slide side to side) and be fitted with a lock to control access to the room.

2.4.5 Closet Location.

TRs shall be dedicated spaces not shared with other functions (i.e., electrical rooms, mechanical rooms, etc). TRs should be located centrally in the area they serve. TRs should be located such that maximum copper cable distance from the patch panel through the structured cabling system to the furthest outlet does not exceed 295 feet. In rehabilitation projects, rooms containing transformers, air handling units, etc., should be avoided if at all possible.

2.4.6 Telephone Backboards.

In new construction and in existing renovation when possible, telephone backboards should cover a minimum of two walls in the TR. Backboards should be ¾-inch thick and 96 inches tall, finished with a fire resistant coating and rigidly attached to the wall to support all attached equipment. When renovating an existing closet that does not have adequate space, the backboard should be sized as large as possible to accommodate the protected entrance terminal (PET) and

110-type blocks. See Figure 2-2: Telecommunications Room Standard Premise Distribution and Figure 2-4: Telecommunications Room Small Facility/Warehouse for sample backboard layouts.

2.4.7 Equipment Racks.

Equipment racks should be floor mounted 19 inches wide located at or near the center of the TR. If mounting requirements for oversize equipment are anticipated, 23 inches may be substituted. In narrow or crowded closets, equipment racks may be floor mounted adjacent to a wall, but should provide a minimum 36 inches space both in front and in back of the rack.

2.4.8 Equipment Cabinets.

Equipment cabinets should be used to mount secure or mission critical equipment or in circumstances where controlled access is desired, such as CATV or CCTV distribution in barracks. Cabinets should provide, at a minimum, sufficient space for current and anticipated future equipment requirements. Equipment cabinets may be floor or wall mounted and should be logically grouped based on the purpose of the equipment they enclose. Air conditioning or fans shall be provided in all equipment cabinets.

2.4.9 Ladder Cable Tray

Channel type ladder cable tray should be used in the TR to provide distribution between the telephone backboard, equipment racks, riser conduits, and the distribution cable tray.

2.4.10 Closet Lighting.

Light fixtures should be mounted a minimum of 102 inches above the finished floor and provide a minimum of 50 foot candles of illumination measured 39 inches above the finished floor.

2.4.11 Closet Climate Control.

Each TR should be independently climate controlled, capable of providing cooling year round (24 hours/day, 365 days/year) to protect all installed electronic equipment. Rooms should be provided with positive atmospheric pressure to exclude dust.

2.4.12 Closet Contaminants.

Information system equipment should not be installed in spaces where moisture, liquid or gaseous spillage, or other contaminants may be present.

2.4.13 Electrical Power.

A minimum of two dedicated 15-ampere, 110-volt alternating current (AC) outlets should be installed with each equipment rack or cabinet to provide power for the installed equipment. Additional utility outlets should be placed on each wall in the telecommunications room.

2.4.14 Voice Communications.

Each TR should have one wall-mounted telephone installed at or near the entry door.

2.5 Grounding

All unclassified TRs should be connected to a single point building ground in accordance with J-STD-607A. Information on grounding of classified facilities can be found in MIL-STD-188-124B and MIL-HNBK-419-A. Figure 2-9 provides a detailed schematic for the building grounding and bonding network. An acceptable grounding system encompasses: cable entrance grounding, the telecommunications main grounding busbar (TMGB), the telecommunications grounding busbar (TGB), the telecommunications bonding backbone (TBB), and the grounding equalizer (GE).

2.5.1 Telecommunications Main Grounding Busbar (TMGB)

A TMGB shall be installed in the cable entrance area, or TEF. The TMGB serves as the main busbar for all telecommunications grounding. The TMGB shall be bonded to the building ground with a bonding conductor equal to or larger that the TBB. Figure 5.4.4.1 of J-STD-607-A provides the bonding conductor sizes. Detailed guidance on the TMGB size, design and application is provided in J-STD-607-A.

Sizing of the TBB	
TBB length linear m (ft)	TBB Size (AWG)
Less than 4 (13)	6
4 - 6 (14 - 20)	4
6-8 (21 -26)	3
8 - 10 (27 - 33)	2
10 - 13 (34 - 41)	1
13 - 16 (42 - 52)	1/0
16 - 20 (53 - 66)	2/0
Greater than 20 (66)	3/0

2.5.2 Building Ground

The building ground should be the primary electrical, life-safety grounding point or system for each building. Typically, a grounding electrode conductor connects the main building ground to the main electrical entrance panel or cabinet. NEC 2002, Article 250 Section III provides guidance on the grounding electrode system and conductor. The resistance-to-ground for a DCO, or main communication node (MCN), should be 5 ohms or less, as indicated in RUS 1751F-802. End user buildings (EUB) and area distribution nodes (ADN) should have a resistance-to-ground of 25 ohms or less, following NEC article 250 and RUS 1751F-802 guidelines. Sites that have resistance-to-ground requirements more stringent than that of NEC 2002 should provide proper supporting documentation and specifications to the designer. Proper documentation includes international, national or local codes, Department of Defense and Department of the Army standards, or manufacturers equipment specifications.

2.5.3 Building Point Of Entrance

NEC defines the point of entrance as the location where “the wire or cable emerges from an external wall, from a concrete floor-slab, or from a rigid metal conduit or an intermediate metal conduit grounded to an electrode in accordance with 800.400(B).”

2.5.3.1 The Telecommunications Entrance Facility (TEF)

The TEF is the space housing the point of entrance of the telecommunications service. The TEF is also the space where the inter- and intra-building backbone facilities join. Telecommunication-related antenna entrances and electronic equipment may also be located in the TEF.

2.5.3.2 Copper Cable Entrance

The OSP copper cable shield, armor, and metallic strength member shall be bonded to the TMGB as close as possible to the building point of entrance with a No. 6 AWG or larger ground wire. The designer should use a non-bonded splice case for the transition from OSP rated cable to interior rated cable, or should indicate that the implementer not install the splice case carry-through bonding conductor. If the designer must extend the OSP copper cable past 50 feet in accordance with NEC 2002 section 800.50, the metallic strength member shall be bonded to the TMGB as close as possible to the conduit egress point with a No. 6 AWG or larger ground wire.

2.5.3.3 Fiber Cable Entrance

The OSP fiber optic cable armor, and metallic strength member shall be bonded to the TMGB as close as possible to the building point of entrance with a No. 6 AWG or larger ground wire. The designer should use a non-bonded splice case for the transition from OSP rated cable to interior rated cable, or should indicate that the implementer not install the splice case carry-through bonding conductor. If the designer must extend the OSP fiber cable past 50 feet in accordance with NEC 2002 section 770.50, the metallic strength member shall be bonded to the TMGB as close as possible to the conduit egress point with a No. 6 AWG or larger ground wire. If inside/outside cable is used, a cable shield isolation gap shall be incorporated.

2.5.4 Copper Protector Block

All OSP copper cables shall be terminated on primary protector blocks, equipped with 5-pin gas protector modules. The protector blocks shall be bonded to the TMGB with a No. 6 AWG or larger ground wire. Blocks shall be UL listed. Place the protector block as close as possible to the TMGB.

2.5.5 Telecommunications Grounding Busbar (TGB)

Each telecommunications room shall have a TGB. The TGB shall be bonded to the TMGB by the 2-5.6Telecommunications bonding backbone (TBB). Detailed guidance on the TGB and TBB size, design, and application is provided in J-STD-607-A.

2.5.6 Telecommunications bonding backbone (TBB)

The TBB is a conductor that connects all TGBs with the TMGB. It reduces or equalizes potential differences between the telecommunications systems to which it is bonded.

2.5.6.1 Grounding Equalizer (GE)

The GE is the conductor that connects the TGBs and the TBB's in multi-floor, multi-closet facilities.

2.5.7 Electrical Power Panel

Electrical power panels collocated with the TMGB or TGB should not be bonded to the TMGB or TGB. The TGB and TMGB should not be bonded to the power panel's alternating current equipment ground or the panel's enclosure.

2.5.8 Electronic Equipment

Electronic equipment shall be bonded to the TGB or TMGB as per the manufacturers installation instructions. The designer and implementer should assume that the equipment requires bonding, unless otherwise stated in the manufacturers literature.

2.5.9 Telecommunications Rack and Supporting Structure

All telecommunications racks and supporting structures shall be bonded to the TGB or TMGB as defined in J-STD-607-A and TIA/EIA-569-A.

2.5.10 Project Design

The ISP designer should include a TMGB and TGB's for locations where the busbar do not exist. The ISP designer should indicate the path, length, and cable size for the TBB, between the TMGB, TGB's, and GE (as needed). The designer should also indicate the path, length, and cable size from the TMGB to the building ground (main electrical service panel). When installing new equipment in a space without a TGB or TGBM, the designer should consider the following:

- The designer should plan for a new TMGB and enough ground cable to connect the equipment to the TMGB and the TMGB to the building ground in the main power panel, if this is the primary or only telecommunications closet for a building.
- The designer should plan for a TGB and enough ground wire to connect the equipment to the TGB and enough TBB to connect the TGB to the TMGB in the primary closet if this is not the main telecommunications closet. Size the TBB in accordance with Figure 5.4.4.1 of J-STD-607-A.
- The designer should also plan for a GE, if there are multiple closets that require TGB's.

2.6 Cable Terminations.

See Figure 2-1-A: Telecommunications Room Entrance and Riser and Figure 2-1-B: Telecommunications Room Horizontal Distribution for typical premise distribution.

2.6.1 Copper Termination.

All copper distribution cable used for voice or data circuits should be terminated at the TR on 110-type (or similar) Cat 6 compliant termination panels mounted in an equipment rack (very small installations, i.e., one or two phones, can use a EIA/TIA Category qualified block).

a. Voice and data cables should normally be terminated on the same patch panel or block and individually identified. Note: in the standard cabling scheme, the designations "voice" and "data" are arbitrary and do not imply that one outlet is better than the other – the outlets are identical in capability.

b. Where physical security is required, or by specific user request, data cable may be terminated in an enclosed 19-inch cabinet to provide enhanced protection for terminations, data equipment, and patching facilities.

2.6.2 Copper Voice Patch Cables.

Voice patch cables should have a standard 8-pin/8-position (RJ45 type) connector on one end and a termination compatible with the incoming voice circuit block or panel on the other end. Although it's not required for voice patch cable to be Cat 6 compliant, it is recommended.

2.6.3 Copper Data Patch Cables.

Data patch cables should be 4-pair, stranded UTP, 24 AWG, Cat 6 cable.

2.6.4 Fiber Optic Termination.

All fiber optic distribution cable should be terminated in rack-mounted patch panels. Duplex patch cables should be used. Where required, and if space allows, all fiber optic cable should be terminated in an enclosed 19-inch cabinet to provide greater protection for terminations, data equipment, and patching

2.6.5 Fiber Optic Patch Cables.

Fiber optic patch cables should be using the same fiber optic cable type and connectors as the patch panels they are interconnecting.

2.7 Telecommunications System Labeling.

The following subparagraphs pertain to patch panel, distribution facilities, and outlet labeling.

2.7.1 Outlet/Patch Panel Labels.

The telecommunications systems labeling should be done in accordance with TIA/EIA 606. All outlets and patch panel positions should be labeled as to their function and with a unique identifier code. All devices, outlet locations, and designations should also appear on the system drawings. As a minimum the following should be reflected in the outlet/patch panel labeling:

- Security Level (if applicable).
- Room Number.
- Alpha or Numeric Designator.
- Labeling should be a minimum of ¼-inch high.

2.7.2 Conformance to Existing Standards.

The labeling system used should conform to any existing labeling, to the Director of Information Management (DOIM) standard, or if neither exists to the method described above. All designations should be done in standard commercial labeling. Handwritten labels should not be used for the final configuration.

2.7.3 Telecommunications Outlet Labeling.

Outlet labeling should be done in accordance with TIA/EIA-606. Each outlet location should be labeled with a unique designator and level of classification, in sequence starting with “A” or “1” and proceeding clockwise around the room. The left or top 8-pin (RJ-45 type), Cat 6 compliant connector should be designated for voice and be labeled "VOICE." The right or bottom 8-pin (RJ-45 type), Cat 6 compliant connector should be designated for data and be labeled "DATA.” All LAN components in the system should also be labeled with similar designations in accordance with TIA/EIA 606. For fiber optic connections, The left or top fiber optic connection should be labeled "A" and the right or bottom fiber optic connection should be labeled "B."

2.7.4 Telecommunications Patch Panel Labeling.

Patch panel labeling should be done in accordance with TIA/EIA 606. Each position should be labeled with a unique designator corresponding to the outlet location. The top or left 8-pin (RJ-45 type), Cat 6 compliant port for each outlet location should be designated for voice and be labeled "VOICE." The bottom or right 8-pin (RJ-45 type), Cat 6 compliant port for each outlet location should be designated for data and be labeled "DATA." Fiber-optic port labeling should be done in accordance with TIA/EIA 606. The left or top connection should be labeled "A." The right or bottom connection should be labeled "B."

2.7.5 Distribution System Labeling.

The distribution system is described in EIA/TIA 606 for pathways. In addition, all transitions and changes in distribution system size and type should be labeled. Each cabinet should be labeled at the top with a unique designation.

2.8 Edge Device for Building.

Power and possibly heating, ventilation, and air-conditioning (HVAC) must be available or obtainable before any equipment is considered.

2.8.1 Selection of Equipment.

Selection of an edge device for an end user building (EUB) should be based on the approved list of network devices, proposed or existing network architecture for that location, and the user requirements. Additional considerations for selecting edge devices are GbE support, LAN Emulation (LANE) support, Multi-Protocol Over Asynchronous Transfer Mode (ATM) (MPOA), and versions supported.

2.8.2 LAN Connectivity and Characteristics.

Defense Data Network (DDN) hosts, mini or mainframe computers, e-mail hosts, and departmental LANs located within EUBs should be directly connected to the network backbone via the appropriate adapter cards in the edge devices and an interface located in the TR. Area Distribution Nodes (ADNs) should also house one-armed routers and LANE service devices when required for support of legacy LANs.

2.8.3 Connection to ADN/Main Communications Node.

The edge device located in the EUB TRs should connect to the switch at the ADN or Main Communications Node (MCN) via OC-3c or higher links, such as GbE. The designer should ensure the edge device is fully compatible with the ADN/MCN data switches.

2.9 Building Entrance Facility.

The building entrance facility (equipment room) is the demarcation point between the outside plant (OSP) cabling and the inside plant distribution cabling.

2.9.1 Protected Entrance Terminals (PET).

2.9.1.1 Protector Modules.

The PET should be equipped to protect the inside plant wiring and equipment from power surges.

2.9.1.2 Copper Termination.

Twisted pair OSP cable is terminated on the PET. See Figure 2-2: Telecommunications Room Standard Premise Distribution for details. Cross connects can then be placed from the PET to the first set of 110-type terminal blocks as needed. The first set of terminal blocks provides connection for all risers and for outlets served by the main TR. For example, in a three-floor building, one tie cable should be terminated on 110-type blocks on the same backboard as the PET; one tie cable should be terminated on 110-type blocks in the 2nd-floor TR; and one tie cable should be terminated on 110-type blocks in the 3rd-floor TR. A tie cable connects a second set of 110-type blocks in each TR to a rack mounted, 8-pin (RJ45 type) connector voice patch panel.

This panel can be patched to the distribution patch panel, which in turn terminates the Cat 6 outlet wiring. Cross connects can be done by the DOIM/Telephone personnel, and jumpers can be installed by the user/Information Mission Area (IMA) department, providing the desired connectivity between the OSP and the inside plant wiring. This design allows maximum flexibility for future moves, adds, and changes.

2.9.1.3 Sheath Limitations.

If the OSP sheath distance from the building entrance point to the PET or fiber optic connector housing location is greater than 50 cable feet; the use of EMT is required.

2.9.1.4 Stencils.

All PETs should be stenciled with the terminal number and cable count.

2.9.2 Fiber Termination Device.

OSP fiber optic cables are terminated on optical patch panels. The inside plant fiber optic riser cables are terminated on optical patch panels in the same or adjacent equipment racks. Patch cables are connected between the patch panels to provide the desired connectivity. All patch panels should be stenciled with the panel number and the cable count.

2.9.3 Placement of Electronics.

Electronic equipment should not be placed in boiler rooms or other environmentally unsound locations. Common-user telecommunications equipment may be installed in the building entrance facility; however, many building entrance facilities do not have the environment control to support the operation of electronic communications equipment. If the building entrance facility does not have environmental control, the electronics should be installed in the primary TR.

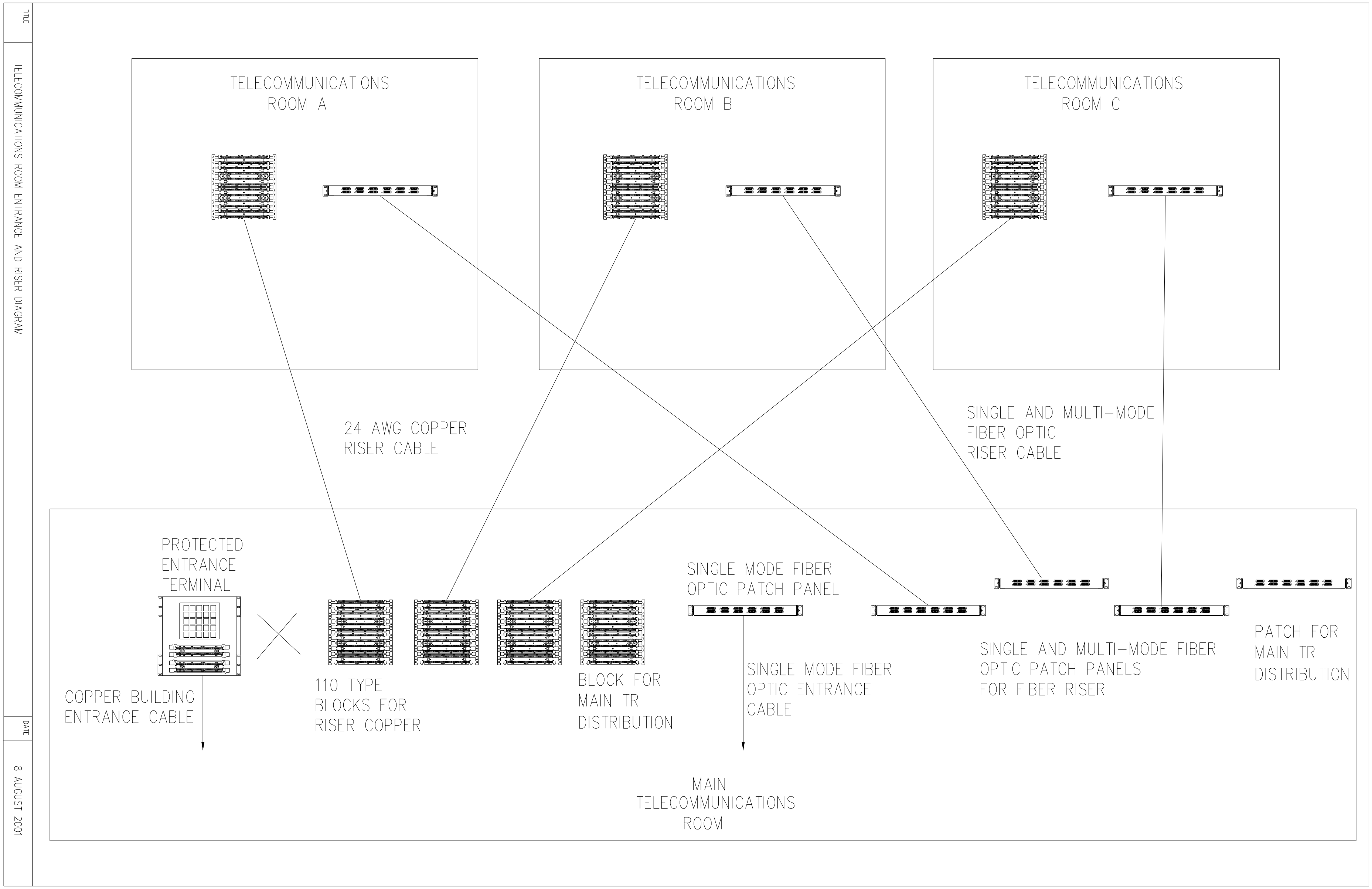

TITLE
TELECOMMUNICATIONS ROOM ENTRANCE AND RISER DIAGRAM
DATE
8 AUGUST 2001
TELECOMMUNICATIONS ROOM A
TELECOMMUNICATIONS ROOM B
TELECOMMUNICATIONS ROOM C
24 AWG COPPER RISER CABLE
SINGLE AND MULTI–MODE FIBER OPTIC RISER CABLE
PROTECTED ENTRANCE TERMINAL
SINGLE MODE FIBER OPTIC PATCH PANEL
COPPER BUILDING ENTRANCE CABLE
110 TYPE BLOCKS FOR RISER COPPER
BLOCK FOR MAIN TR DISTRIBUTION
SINGLE MODE FIBER OPTIC ENTRANCE CABLE
SINGLE AND MULTI–MODE FIBER OPTIC PATCH PANELS FOR FIBER RISER
PATCH FOR MAIN TR DISTRIBUTION
MAIN TELECOMMUNICATIONS ROOM

Figure 2-1-A: Telecommunications Room Entrance and Riser

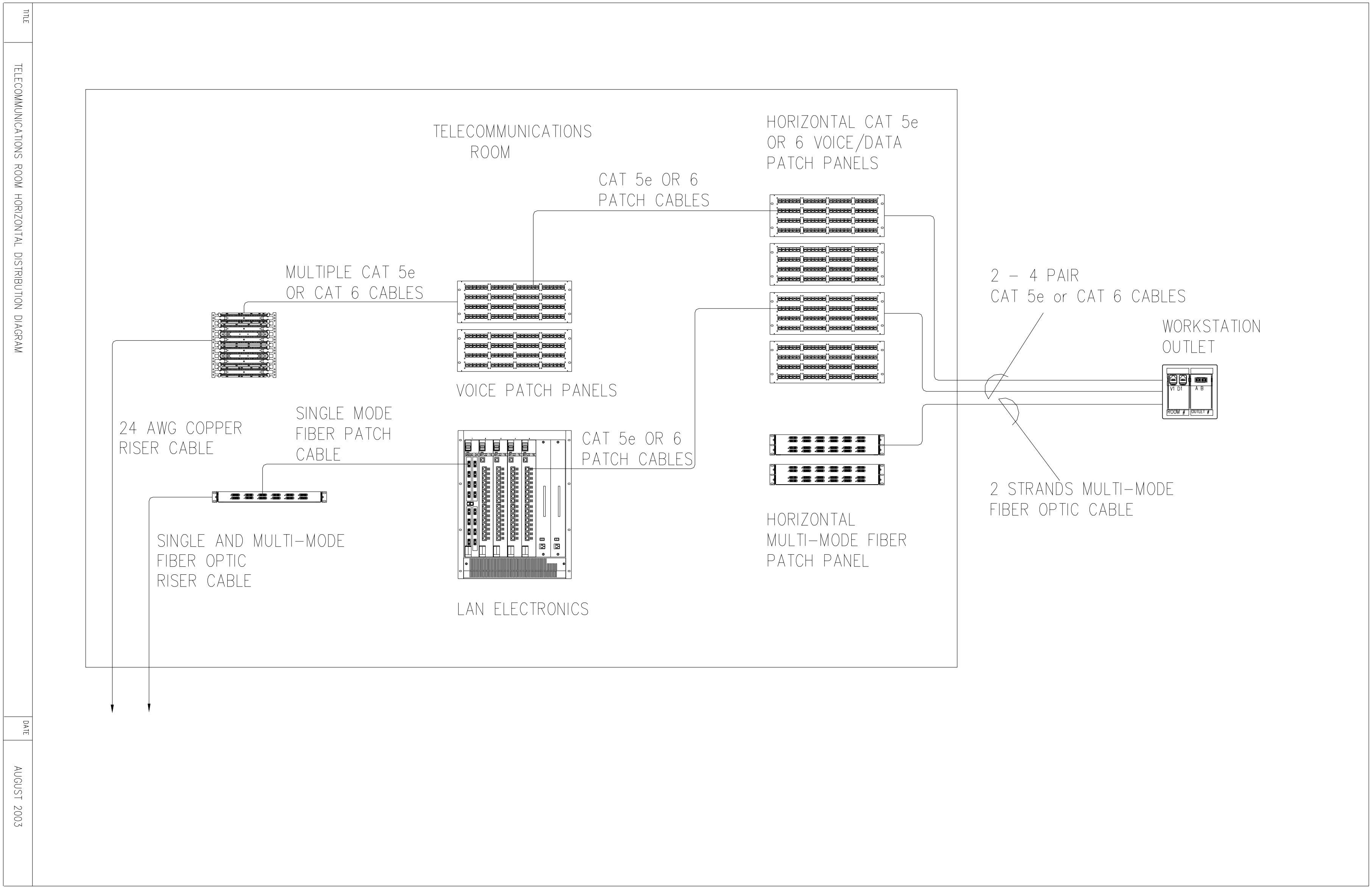

TITLE
TELECOMMUNICATIONS ROOM HORIZONTAL DISTRIBUTION DIAGRAM
DATE
AUGUST 2003
TELECOMMUNICATIONS ROOM
HORIZONTAL CAT 5e OR 6 VOICE/DATA PATCH PANELS
CAT 5e OR 6 PATCH CABLES
MULTIPLE CAT 5e OR CAT 6 CABLES
2 – 4 PAIR CAT 5e or CAT 6 CABLES
WORKSTATION OUTLET
VT D1
A B
ROOM #
OUTLET #
VOICE PATCH PANELS
24 AWG COPPER RISER CABLE
SINGLE MODE FIBER PATCH CABLE
CAT 5e OR 6 PATCH CABLES
2 STRANDS MULTI–MODE FIBER OPTIC CABLE
SINGLE AND MULTI–MODE FIBER OPTIC RISER CABLE
HORIZONTAL MULTI–MODE FIBER PATCH PANEL
LAN ELECTRONICS

Figure 2-1-B: Telecommunications Room Horizontal Distribution

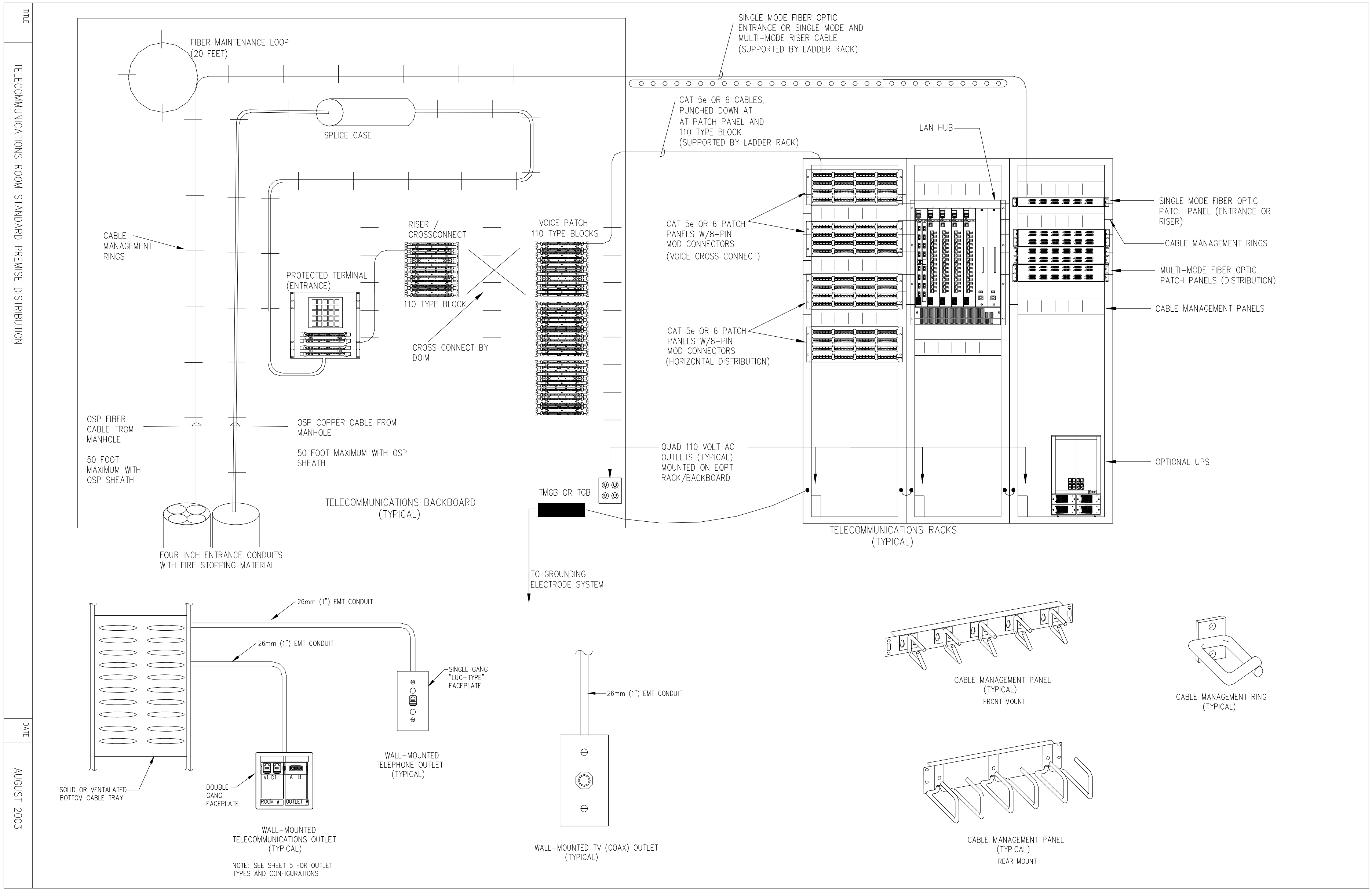


Figure 2-2: Telecommunications Room Standard Premise Distribution

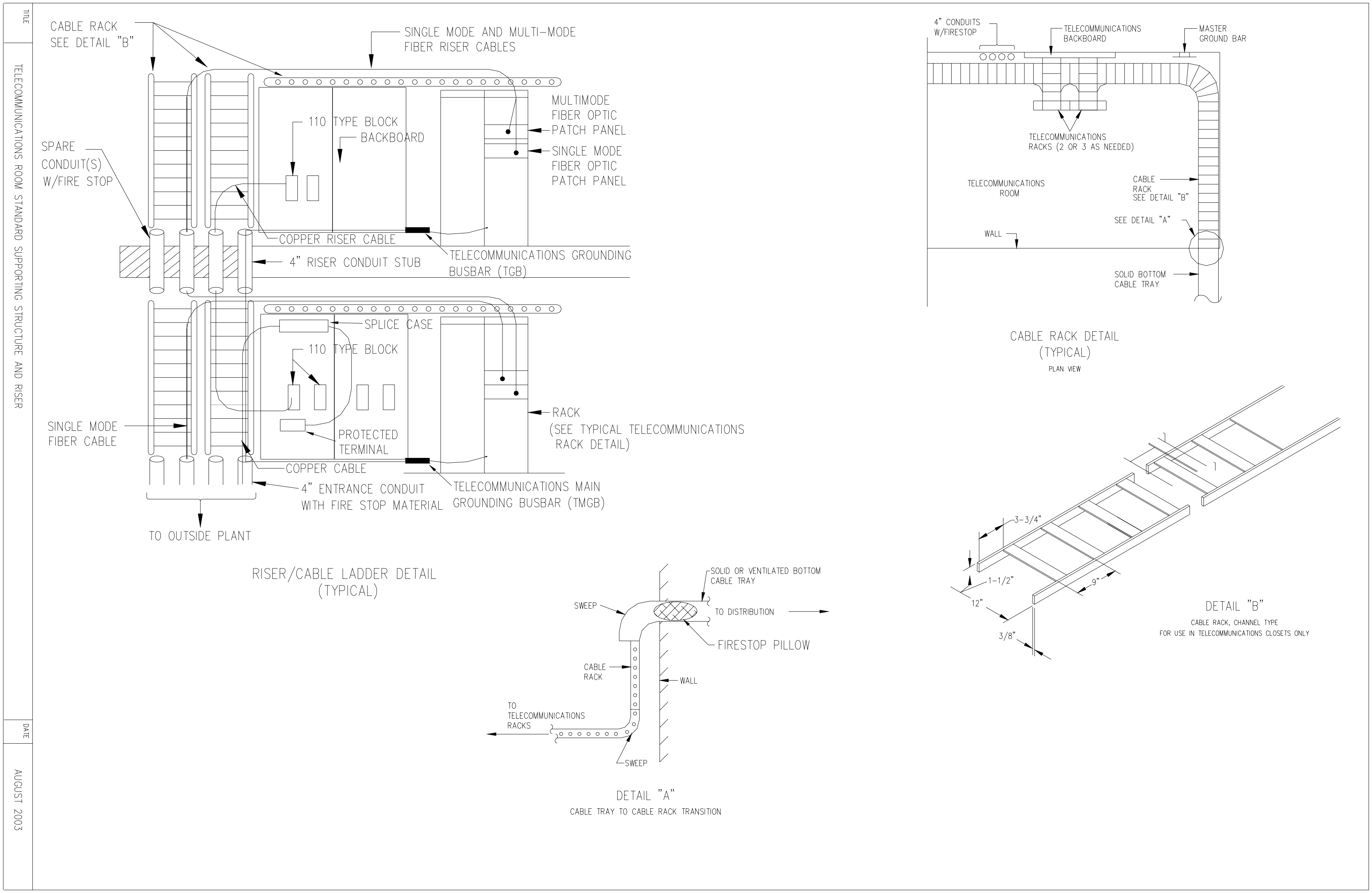


Figure 2-3: Telecommunications Room Standard Supporting Structure and Riser

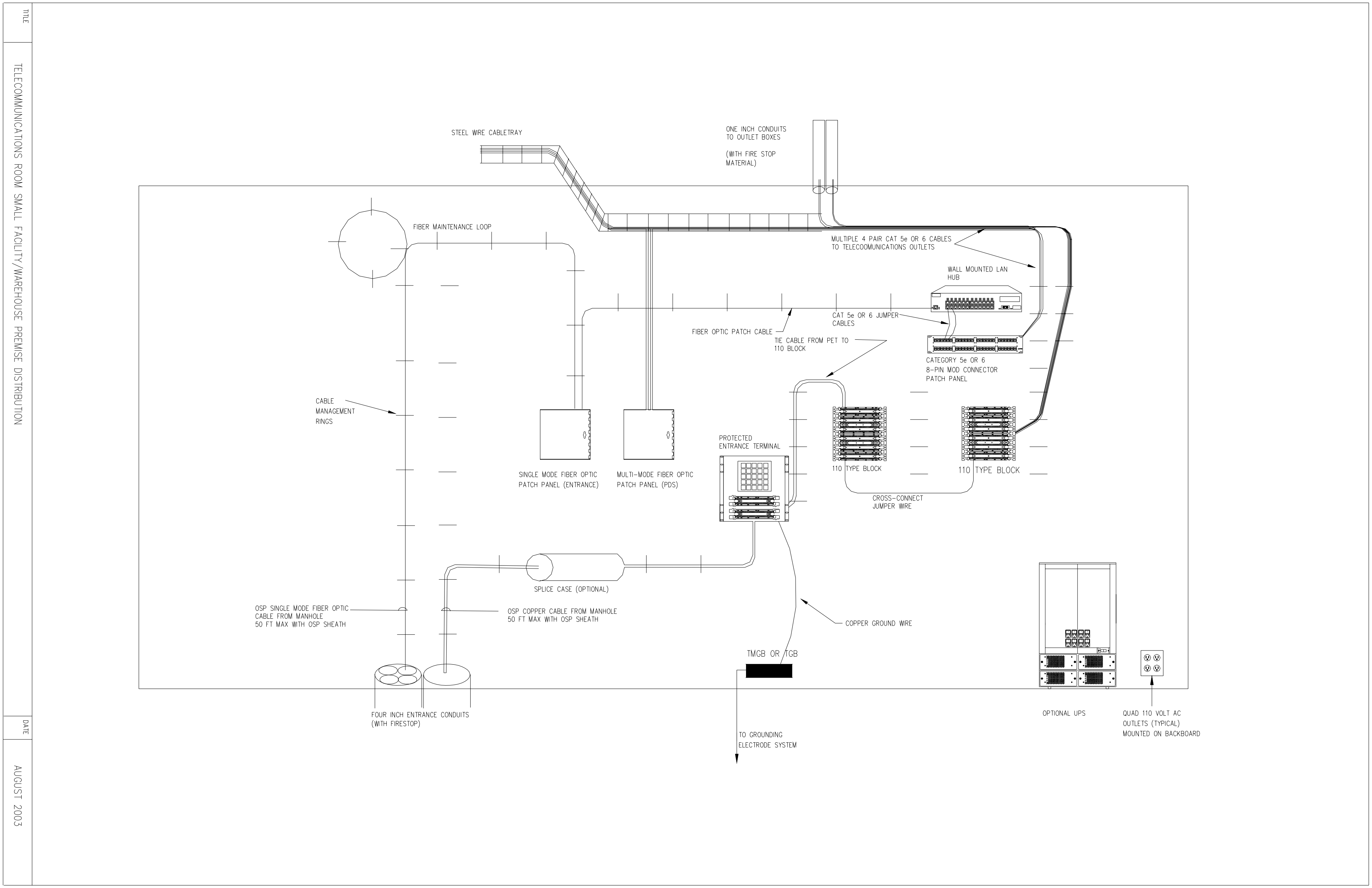

TITLE
TELECOMMUNICATIONS ROOM SMALL FACILITY/WAREHOUSE PREMISE DISTRIBUTION
DATE
AUGUST 2003
STEEL WIRE CABLETRAY
ONE INCH CONDUITS TO OUTLET BOXES
(WITH FIRE STOP MATERIAL)
FIBER MAINTENANCE LOOP
MULTIPLE 4 PAIR CAT 5e OR 6 CABLES TO TELECOOMUNICATIONS OUTLETS
WALL MOUNTED LAN HUB
CAT 5e OR 6 JUMPER CABLES
FIBER OPTIC PATCH CABLE
TIE CABLE FROM PET TO 110 BLOCK
CATEGORY 5e OR 6 8-PIN MOD CONNECTOR PATCH PANEL
CABLE MANAGEMENT RINGS
PROTECTED ENTRANCE TERMINAL
SINGLE MODE FIBER OPTIC PATCH PANEL (ENTRANCE)
MULTI-MODE FIBER OPTIC PATCH PANEL (PDS)
110 TYPE BLOCK
110 TYPE BLOCK
CROSS-CONNECT JUMPER WIRE
SPLICE CASE (OPTIONAL)
OSP SINGLE MODE FIBER OPTIC CABLE FROM MANHOLE 50 FT MAX WITH OSP SHEATH
OSP COPPER CABLE FROM MANHOLE 50 FT MAX WITH OSP SHEATH
COPPER GROUND WIRE
TMGB OR TGB
FOUR INCH ENTRANCE CONDUITS (WITH FIRESTOP)
TO GROUNDING ELECTRODE SYSTEM
OPTIONAL UPS
QUAD 110 VOLT AC OUTLETS (TYPICAL) MOUNTED ON BACKBOARD

Figure 2-4: Telecommunications Room Small Facility/Warehouse

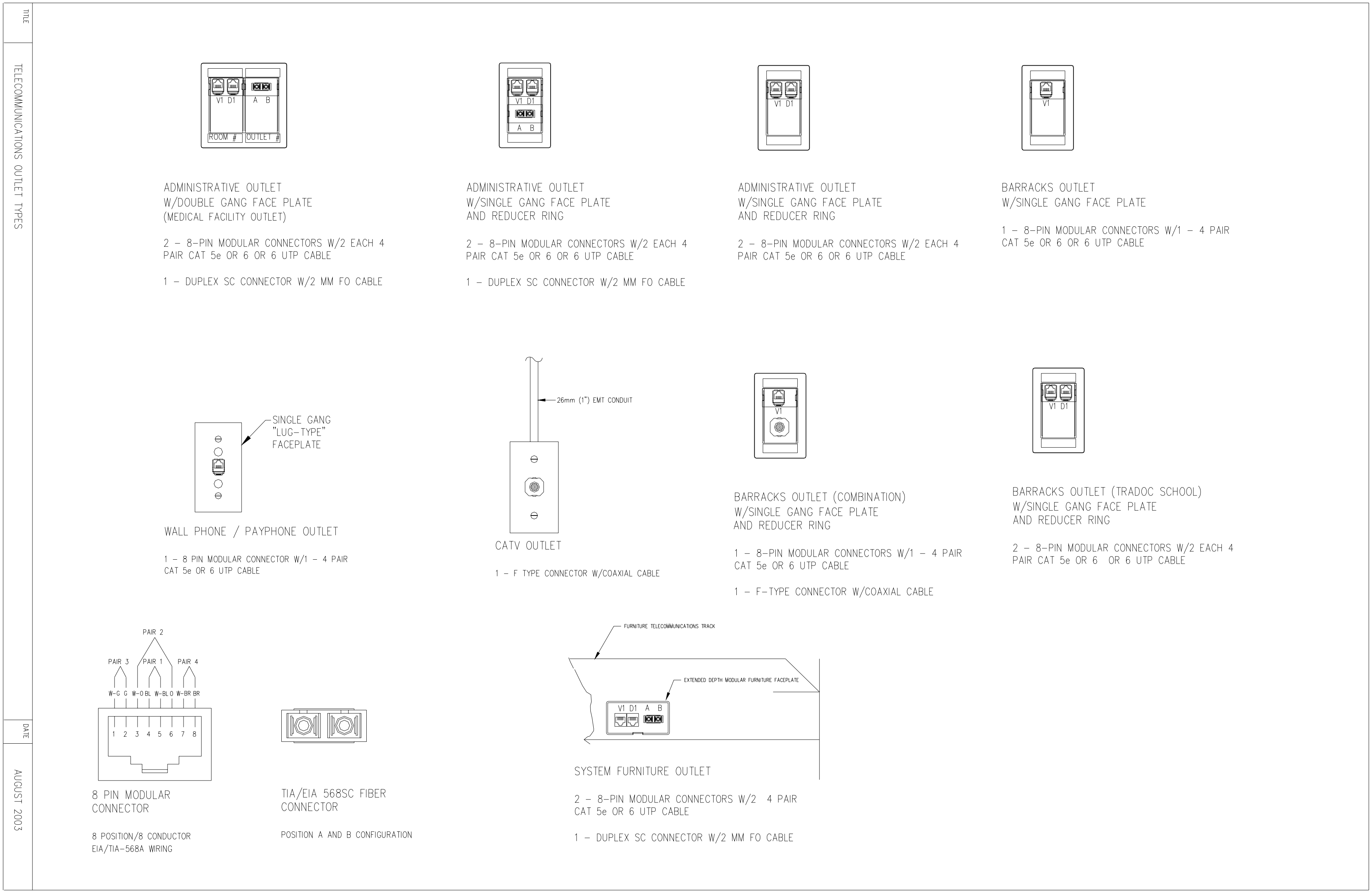
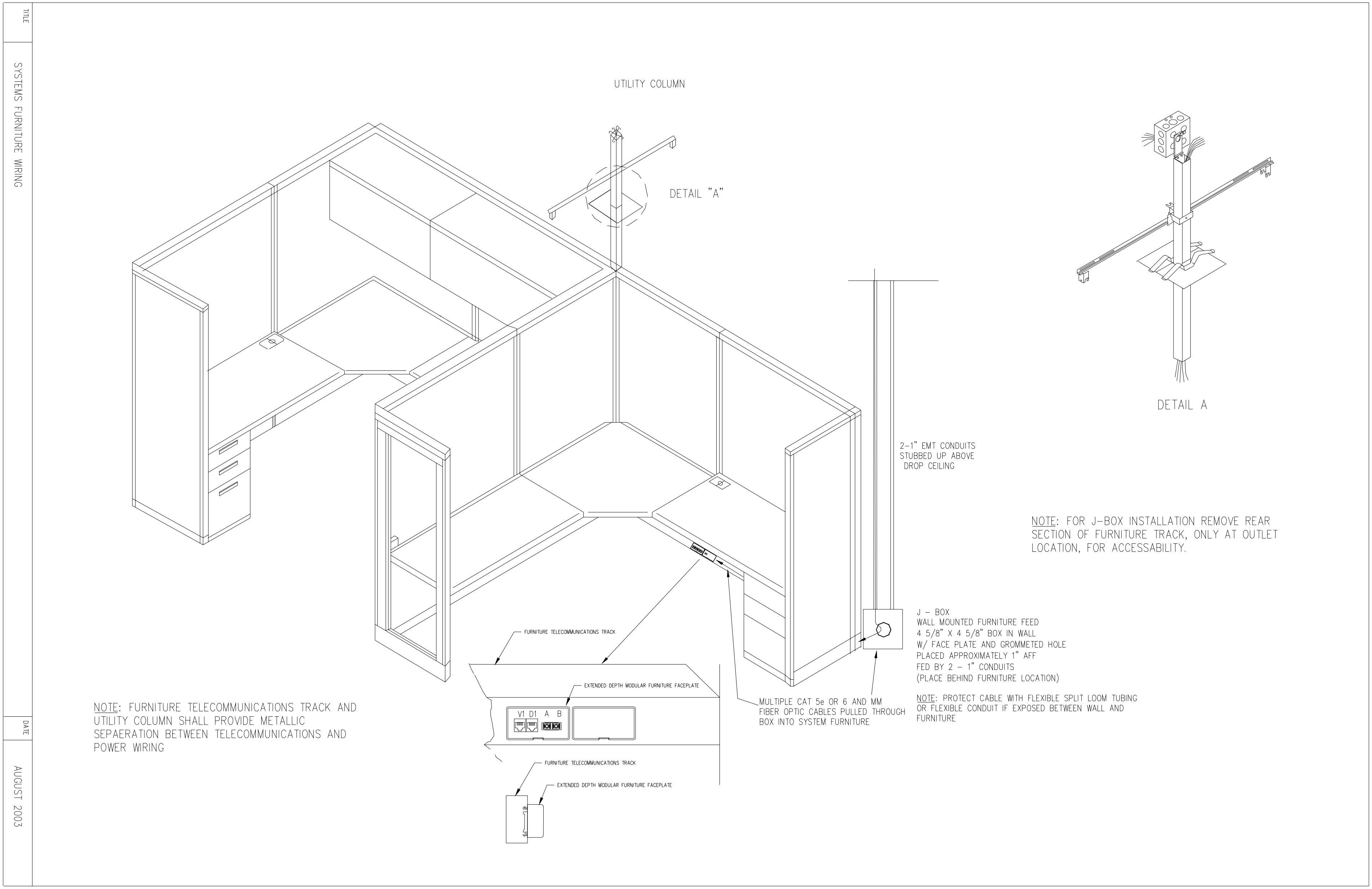

TITLE
TELECOMMUNICATIONS OUTLET TYPES
DATE
AUGUST 2003
V1 D1
A B
ROOM #
OUTLET #
ADMINISTRATIVE OUTLET
W/DOUBLE GANG FACE PLATE
(MEDICAL FACILITY OUTLET)
2 – 8–PIN MODULAR CONNECTORS W/2 EACH 4 PAIR CAT 5e OR 6 OR 6 UTP CABLE
1 – DUPLEX SC CONNECTOR W/2 MM FO CABLE
V1 D1
A B
ADMINISTRATIVE OUTLET
W/SINGLE GANG FACE PLATE
AND REDUCER RING
2 – 8–PIN MODULAR CONNECTORS W/2 EACH 4 PAIR CAT 5e OR 6 OR 6 UTP CABLE
1 – DUPLEX SC CONNECTOR W/2 MM FO CABLE
V1 D1
ADMINISTRATIVE OUTLET
W/SINGLE GANG FACE PLATE
AND REDUCER RING
2 – 8–PIN MODULAR CONNECTORS W/2 EACH 4 PAIR CAT 5e OR 6 OR 6 UTP CABLE
V1
BARRACKS OUTLET
W/SINGLE GANG FACE PLATE
1 – 8–PIN MODULAR CONNECTORS W/1 – 4 PAIR CAT 5e OR 6 OR 6 UTP CABLE
SINGLE GANG "LUG–TYPE" FACEPLATE
WALL PHONE / PAYPHONE OUTLET
1 – 8 PIN MODULAR CONNECTOR W/1 – 4 PAIR CAT 5e OR 6 UTP CABLE
26mm (1") EMT CONDUIT
CATV OUTLET
1 – F TYPE CONNECTOR W/COAXIAL CABLE
V1
BARRACKS OUTLET (COMBINATION)
W/SINGLE GANG FACE PLATE
AND REDUCER RING
1 – 8–PIN MODULAR CONNECTORS W/1 – 4 PAIR CAT 5e OR 6 UTP CABLE
1 – F–TYPE CONNECTOR W/COAXIAL CABLE
V1 D1
BARRACKS OUTLET (TRADOC SCHOOL)
W/SINGLE GANG FACE PLATE
AND REDUCER RING
2 – 8–PIN MODULAR CONNECTORS W/2 EACH 4 PAIR CAT 5e OR 6 OR 6 UTP CABLE
PAIR 2
PAIR 3
PAIR 1
PAIR 4
W–G G W–O BL W–BL O W–BR BR
1 2 3 4 5 6 7 8
8 PIN MODULAR CONNECTOR
8 POSITION/8 CONDUCTOR EIA/TIA–568A WIRING
TIA/EIA 568SC FIBER CONNECTOR
POSITION A AND B CONFIGURATION
FURNITURE TELECOMMUNICATIONS TRACK
EXTENDED DEPTH MODULAR FURNITURE FACEPLATE
V1 D1 A B
SYSTEM FURNITURE OUTLET
2 – 8–PIN MODULAR CONNECTORS W/2 4 PAIR CAT 5e OR 6 UTP CABLE
1 – DUPLEX SC CONNECTOR W/2 MM FO CABLE

Figure 2-5: Telecommunications Outlet Types


TITLE
SYSTEMS FURNITURE WIRING
DATE
AUGUST 2003
UTILITY COLUMN
DETAIL "A"
DETAIL A
2-1" EMT CONDUITS
STUBBED UP ABOVE
DROP CEILING
FURNITURE TELECOMMUNICATIONS TRACK
EXTENDED DEPTH MODULAR FURNITURE FACEPLATE
V1 D1 A B
FURNITURE TELECOMMUNICATIONS TRACK
EXTENDED DEPTH MODULAR FURNITURE FACEPLATE
MULTIPLE CAT 5e OR 6 AND MM
FIBER OPTIC CABLES PULLED THROUGH
BOX INTO SYSTEM FURNITURE
J - BOX
WALL MOUNTED FURNITURE FEED
4 5/8" X 4 5/8" BOX IN WALL
W/ FACE PLATE AND GROMMETED HOLE
PLACED APPROXIMATELY 1" AFF
FED BY 2 - 1" CONDUITS
(PLACE BEHIND FURNITURE LOCATION)

NOTE: FOR J-BOX INSTALLATION REMOVE REAR SECTION OF FURNITURE TRACK, ONLY AT OUTLET LOCATION, FOR ACCESSABILITY.

NOTE: FURNITURE TELECOMMUNICATIONS TRACK AND UTILITY COLUMN SHALL PROVIDE METALLIC SEPAERATION BETWEEN TELECOMMUNICATIONS AND POWER WIRING

NOTE: PROTECT CABLE WITH FLEXIBLE SPLIT LOOM TUBING OR FLEXIBLE CONDUIT IF EXPOSED BETWEEN WALL AND FURNITURE

Figure 2-6: Systems Furniture Wiring

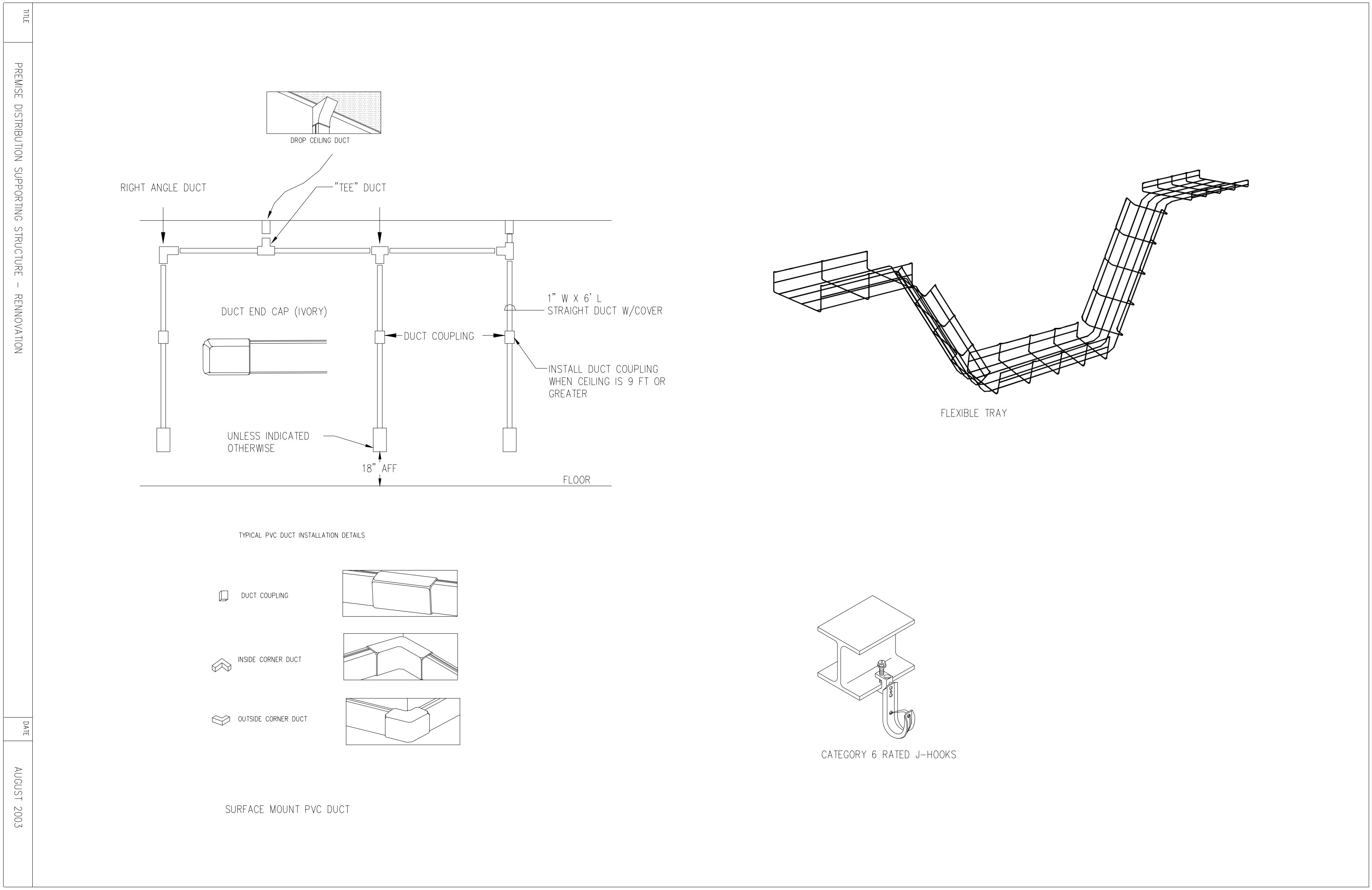
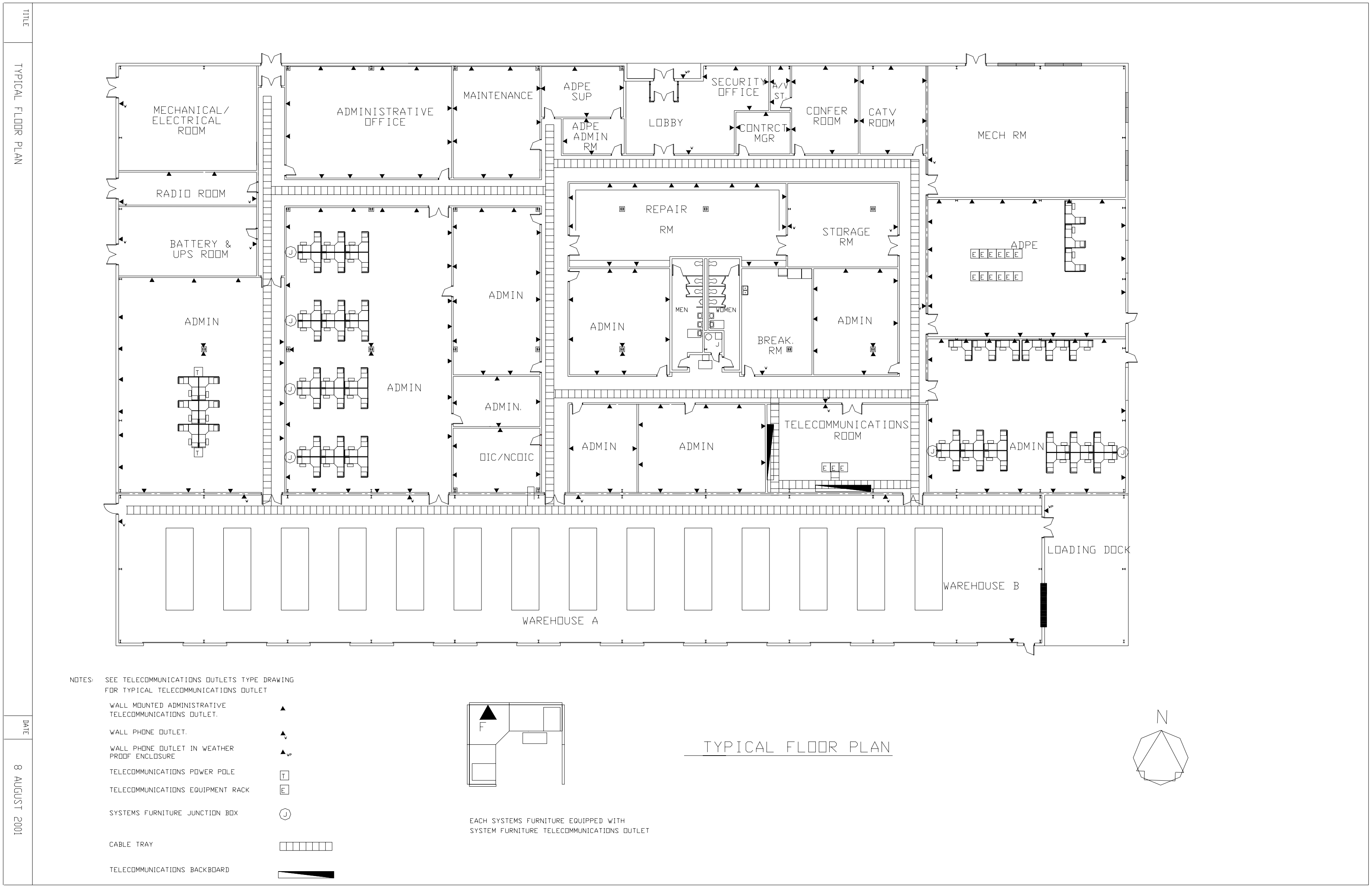


Figure 2-7: Premise Distribution Supporting Structure - Renovations



NOTES: SEE TELECOMMUNICATIONS OUTLETS TYPE DRAWING FOR TYPICAL TELECOMMUNICATIONS OUTLET

EACH SYSTEMS FURNITURE EQUIPPED WITH SYSTEM FURNITURE TELECOMMUNICATIONS OUTLET

Figure 2-8: Typical Floor Plan

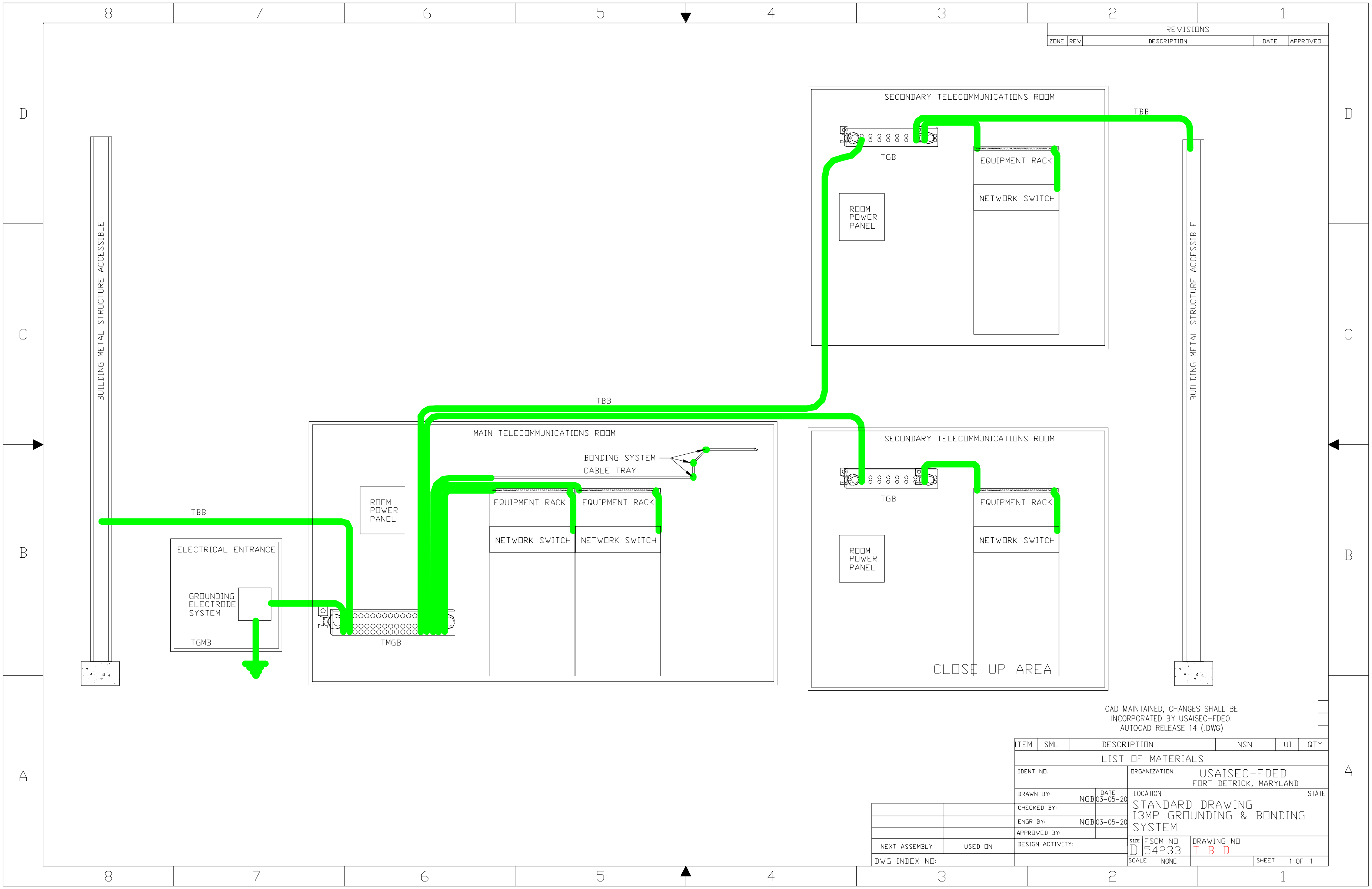


Figure 2-9 Grounding System

3.0 OUTSIDE PLANT.

An overall schematic for OSP sizing of duct and cable is provided in Figure 3-3: OSP Infrastructure Standards. Much of the OSP work references Rural Utilities Service (RUS) standards that are maintained by USDA. The RUS bulletins referenced in this section have been reorganized into 7CFR regulation parts 1753 and 1755. Most of the RUS bulletins are still available in electronic format. The 7CFR Regulation and the RUS Bulletins are available at (http://www.usda.gov/rus/telecom/publications/publications.htm).

3.1 Environmental and Historical Considerations.

Most military installations have areas that may be affected by environmental, historical, or archeological restrictions. Environmental hazards may include toxic waste, fuel spillage/leakage, asbestos, unexploded ordinances, etc. Wildlife preservation may be another area of concern at some sites. Compliance with historical restrictions will require special engineering considerations (type of exterior facing, mounting of terminals, placement of pedestals, etc.).

3.1.1 Price of Conformance.

Although these issues may not appear to have a high impact on the engineering solution, the price of conformance to site restrictions may add considerable cost to the project. Special conditions should be discussed with the DOIM and agreements documented.

3.2 Construction/Installation Alternatives.

3.2.1 General Installation.

The following paragraphs pertain to cable routing considerations.

3.2.1.1 Road Crossings.

The cable route should be planned to cross the road only as necessary to serve subscribers without the use of aerial inserts. Such crossings could be constructed by cutting or sawing perpendicularly across the road, by trenching perpendicularly across the road, by directional boring under the road, or by pipe pushing under the road. Since road crossings are often undesirable and expensive, construction route planning personnel should select the side of the paved road for the most general routing of the cable, which will result in the fewest crossings.

3.2.1.2 Right-of-Ways.

Permission should be obtained from Department of Transportation authorities at locations where public right-of-ways are used. Possible highway improvements, such as road widening, should be considered in planning the construction route. Future roadwork can result in costly telecommunications plant rearrangements or relocations. Additional lead-time is required to obtain permission for public right-of-ways. Detailed drawings showing proposed route, depths, and other pertinent information are required and should be furnished to the approving authorities for review far in advance of anticipated installation. Alternate designs should be explored in case the right-of-way is denied.

3.2.1.3 OSP Cable Placement Options.

An underground (concrete encased manhole and duct) system should be used for placement of outside cable plant in new construction and rehabilitation, within the site cantonment areas, unless otherwise specified. Manhole and duct should be utilized in accordance with the RUS bulletins within congested areas, under all vehicle crossings, around sweeps, bends and utilities, etc. Direct buried and aerial cable plant systems should not be used except for range cables or other long runs through undeveloped areas, in cases where underground systems cannot be installed or in conformance to local mandates.

3.2.2 Underground (Manhole/Duct).

Supporting documentation for design and construction of manhole and duct is found in RUS Bulletin 1751F-643/RUS Form 515C (http://www.usda.gov/rus/telecom/publications/1751f643.pdf), RUS Bulletin 1751F-644 (http://www.usda.gov/rus/telecom/publications/1751f644.pdf), REA Bulletin 345-151, and TIA/EIA-758, Customer Owned outside Plant Telecommunications Cabling Standard.

3.2.2.1 Manholes.

See Figure 3-6: Manhole Typical for additional details.

2.3.5.6.53.2.2.1.1 Types.

Typical manhole size should be 12 feet (L) x 6 feet (W) x 7 feet (H). Precast, multidirectional manholes should be used. Splayed manholes would be beneficial near MCN/ADN where large cables are engineered and where future duct expansion is expected. See Figure 3-6: Manhole Typical for a butterfly schematic of a typical manhole.

2.3.5.6.63.2.2.1.2 Oversized Manholes for Route Diversity Splicing.

To avoid catastrophic loss of service in case of building destruction, fibers providing physical route diversity should not be routed through the MCN or ADNs. These cables should be spliced in the manhole and routed to their ultimate destination without entering the MCN/ADN. The manhole placed outside an MCN/ADN should be oversized to allow for this additional splicing.

2.3.5.6.73.2.2.1.3 Basic Layout.

Measurements between manholes are from lid to lid (center-to-center (CC)). Measurements from manholes to buildings, to pedestals, riser poles, etc. are from the manhole lid to the outside wall, bottom of pole, etc. (center-to-point (CP)). New manholes should be placed to support the locations of junction points, offsets, load points, and curvature in the duct line. New manholes should be placed 600 feet apart. However, consideration should be given to varying this distance to make maximum use of the duct system. For example, if increasing or shortening the distance by 100 feet will allow installation of the ducts to avoid a building or other obstruction in the intended path, then the adjustment should be made if it does not violate the cable reel lengths or pulling tension for the cables to be installed.

2.3.5.6.83.2.2.1.4 Accessories.

Each new manhole should be equipped with a sump, pull irons, ground rod, bonding ribbon, cable racks and hooks.

3.2.2.1.4.1 Sump.

A sump should be cast into the floor of the manhole. The floor should slope toward the sump to provide drainage from all areas into the sump. The sump should be approximately 13 inches square and 4 inches deep, equipped with a plugged drain, and covered with a removable perforated or punched-steel plate to permit drainage. The cover should be fastened to the housing by a chain or a hinge.

3.2.2.1.4.2 Pull Irons.

Cable pull irons should be installed on the wall opposite each main conduit entrance location 3-1/2 inches to 9 inches from the floor of the manhole in line with the conduit entrance. The pull irons should be placed and embedded during the construction of the manhole wall.

3.2.2.1.4.3 Ground Rod.

A 5/8-inch by 8-foot galvanized steel ground rod should be installed in the floor of each manhole. Four inches of the rod, plus or minus 1/2 inch, should extend above the finished floor level. The rod should not enter the manhole more than 3 inches nor less than 2 inches out from the vertical surface of the adjacent wall. All manhole splices should be bonded to the manhole ground. In existing manholes new ground rods and/or bonding ribbon should be designed at each splice location if none presently exist. Note: Pull throughs require no grounding.

3.2.2.1.4.4 Bonding Ribbon.

Bonding ribbon should be installed in all new manholes. The bonding ribbon should be attached to all rack anchors and be precast into the manholes. The bonding ribbon should be attached to the manhole ground rod.

3.2.2.1.4.5 Hardware.

A minimum of five cable racks, each containing 47 hook spaces mounted vertically, should be provided on each long wall. End wall manhole racks should be provided at the T-end of multi-directional manholes. Corner racks should be provided at the in-line end of the manhole. Racks should set out from the wall a minimum of 3 inches. Each cable rack should be equipped with hooks to support all existing/new cable or if there are no existing/new cables, each rack should be equipped with two cable hooks (minimum length 7 and 1/2 inches). All racks and hooks should be of galvanized metal or non-corrosive materials.

2.3.5.6.93.2.2.1.5 Stencil.

All new manholes should be stenciled with a number designated by the DOIM.

3.2.2.2 Handholes.

The installation of handholes is not suggested. The cost savings are minimal and do not overcome the limited work space and future problems experienced with handhole installation. The preferred solution is the installation of a full-size manhole. Handholes may be installed if the space is limited or under other extenuating circumstances.

3.2.2.3 Duct.

The type of duct for new installation should be PVC, Schedule B, EB, C, or DB. Schedule B or EB should be used in installations where the duct is concrete encased. Since Schedule B or EB is less robust, care should be taken to ensure that the thin-wall duct is properly supported by spacers, a minimum of one spacer every 10 feet or in accordance with manufacture’s specifications and is not damaged (cracked or crushed) prior to or during installation. Schedule C or DB duct should be used for applications where the duct is buried rather than encased in concrete.

2.3.5.6.10 3.2.2.3.1 Minimum Duct Sizing.

The minimum sizing for new duct is shown in Figure 3-3: OSP Infrastructure Standard. All duct sizes should be designed to allow for current cable, new cable under this effort, and 50 percent growth. Minimum sizing is listed below.

a. **Duct between the cable vault and the first manhole should be based upon the size of the switch and the number of outside cable pairs served from the switch location.**
b. **Main duct runs should be a minimum of 6-way, 4-inch (two of which are subduct).**
c. **Lateral duct runs should be a minimum of 4-way, 4-inch (one of which is subduct).**
d. **Building entrance ducts should be a minimum of 2-way, 4-inch (one of which is subduct).**

3.2.2.3.2 Depth of Cover.

At least 24" of cover is required above the top of the duct or duct encasement. Less cover is required under roads or sidewalks (if duct is concrete encased). See Figure 3-5: Conduit Placement and Cut & Resurface for details.

3.2.2.3.3 Trench Width.

To install ducts, the trench width depends on the number of ducts, size of ducts, arrangement of ducts, and space around ducts (at least 2"). Additional width may be required to work in deep trenches or with large count duct banks. See Figure 3-5: Conduit Placement and Cut & Resurface for details.

3.2.2.3.4 New Duct Placement.

In a new duct run, the duct should be swept down into the lower duct window. This practice will allow for easier expansion of the duct run in the future.

3.2.2.3.5 Rerouting of Existing Duct.

Existing duct should be joined to new manholes (precast or cast-in-place) by rerouting the designated ducts from the demolished or abandoned manhole to the new. Rerouting should begin far enough back from the old manhole to allow for standard bending radius and pulling tension. Continuity of operations on the affected cables should be maintained during the duct rerouting actions.

3.2.2.3.6 Reinforced Duct Placement.

New duct, installed to reinforce an existing duct bank, should be placed above the existing duct bank if the minimum top cover of 24 inches can be maintained. If there is not sufficient top cover available, the new duct should be placed beside the existing duct bank.

3.2.2.3.7 Concrete Encasement.

Concrete encased duct or galvanized steel pipe should be placed under all paved road surfaces and certain heavy-traffic non-surfaced roads. The encasement/pipe should be extended a minimum of 6 feet beyond the roadbed for all road crossings on ranges. In accordance with the referenced standards, PVC duct should also be encased in concrete at all sweeps or bends; at stream or drainage ditch crossings or other areas subject to washout, and in runs parallel to streets, highways or road surfaces where the top cover is less than 30 inches. For consistency, the contractor should use only one brand of cement that conforms to RUS Bulletin 1751F-644 (http://www.usda.gov/rus/telecom/publications/1751f644.pdf).

3.2.2.3.8 Rock.

Rock is defined as boulders measuring ½ cubic yard or more or other material, such as rock in ledges, bedded deposits, unstratified masses and conglomerate deposits, or below ground concrete masonry structures, that cannot be moved without systematic drilling and blasting or the use of a rock saw. Pavements should not be considered as rock. Excavate rock to a minimum of 4 inches below the trench depths required to place duct bank or cable. Backfill the rock excavation and all excess trench excavation with a 4-inch cushion of sand prior to placing the duct or cable.

3.2.2.3.9 Unstable Soil.

When wet or otherwise unstable soil incapable of properly supporting this conduit is encountered in the trench bottom, remove such soil to the depth required and backfill the trench to trench bottom grade, with coarse sand or fine gravel.

3.2.2.3.10 Bends and Sweeps.

Accomplish changes in direction of runs exceeding a total of 10 degrees, either vertically or horizontally, by long sweeping bends having a minimum radius of 25 feet. In no instance should the total of all bends and sweeps in a duct run exceed 180 degrees. Manufactured bends may be used on subsidiary/lateral conduit at the riser pole or building entrance. Long sweeps may be made up of one or more curved or straight sections and/or combinations thereof. Manufactured bends should have a minimum radius of 24 inches for all conduits 3 inches in diameter or larger. Conduits should terminate in bell ends at point of entrance into the manholes and buildings. All bends and sweeps should be concrete encased to protect the duct from the pressures developed while pulling cables.

3.2.2.3.11 Pull String/Rope.

Pull string should be installed in each new conduit or innerduct/subduct. A minimum of 5 feet of pull string should be provided at each end of the conduit. The pull string should be coiled and secured to the wall.

3.2.2.3.12 Plugs.

All ducts subduct and/or innerduct, whether main or subsidiary runs, not scheduled for immediate use should be plugged using acceptable duct plugs or plugging compound. Concrete is not acceptable for plugging ducts.

3.2.2.3.13 Galvanized Steel Pipe (GSP).

For road crossing using the cut and restore method, GSP should generally only be used if the local Department of Public Works (DPW) or DOIM request that trenches not be left open across roadways for an extended duration (to allow for concrete to harden). Otherwise, concrete encased duct should be used. GSP should be used to push under railroad crossings. The GSP should be 12 inches or greater for pushing under commercial railroad crossings and for multi-duct conduit runs under non-commercial railroad beds. One four-inch GSP can be installed under non-commercial railroad beds in single conduit applications. See Figure 3-5: Conduit Placement and Cut & Resurface for details on railroad crossing.

3.2.2.3.14 Split Duct.

Split Duct is designed for use on a long cable run (normally fiber optic) where the cable is placed in the open duct while the duct and trench are still open. Split Duct should be used for all road crossings only after 1/5 of the cable reel length for cables greater than 1 inch in diameter, and 1/3 of the cable reel length for cables less than 1inch in diameter, is utilized in each unspliced span (up to 5,000 feet). Normal conduit should be utilized at all other areas.

3.2.2.3.15 Rod/Mandrel/Slug/Clean Ducts or Conduits.

Rodding a duct entails inserting or pushing a rod into the duct to determine the length of the duct, locate the other end of the duct, determine if the duct is usable or blocked, or insert a pull string in the duct. Mandrelling a duct consists of pulling a mandrel or slug through the duct to clean any mud, sand, or dirt out of the duct. Mandrelling also insures that the duct diameter is intact and available for installation of cable. The mandrel's diameter (1/4" less than the duct inside diameter) depends on the type and size of the ducts. **Do not mandrel the ducts if existing cables are in the duct.**

Existing vacant ducts, without pull strings, that are to be used in new cable installation should be rodded and mandrelled to detect any obstructions, collapsed ducts, or duct inconsistencies and to place a pull string. Vacant duct, with pull strings, which are to be used in new cable construction should be cleaned with a slug/mandrel prior to the installation of cable.

3.2.2.4 Subduct/Innerduct.

Subduct should be used when installing new conduit systems. Each subduct should provide four 1-1/2 inch conduits in the space that is normally occupied by a 4-inch conduit. Each pathway should be provided with pull string. One out of every 4 new ducts should be subduct.

Innerduct is used in existing conduit systems, in GSP or split GSP, or in open trenches for direct buried fiber optic cables. The Government's preference is to use the rigid type innerduct with pull string instead of the flexible innerduct. The type and size of existing conduit should determine the number of innerducts. Typically, four 1-inch innerducts are placed in a 4-inch conduit. Although more innerducts will physically fit in a 4-inch duct, the twisting and intertwining of the innerducts make installation impractical.

3.2.3 Direct Buried.

Supporting documentation for buried cable installation is available in RUS Bulletins 1751F-640 (http://www.usda.gov/rus/telecom/publications/1751f640.pdf), 641 (http://www.usda.gov/rus/telecom/publications/1751f641.pdf), and 642 (http://www.usda.gov/rus/telecom/publications/1751f642.pdf) and TIA/EIA-758, Customer Owned Outside Plant Telecommunications Cabling Standard.

3.2.3.1 Type of Cable.

Rodent protected cable should be used for buried applications and at locations where there is a problem with rodents damaging underground cables. Typically, all non-rodent proof direct buried cables should be placed in buried innerduct when the outer diameter of the cable is smaller than a gopher's bite dimensions.

3.2.3.2 Warning Tape.

Buried cable warning tape should be used for all direct buried applications (open trenching and plowing). The tape should be installed 12 inches above the cable.

3.2.3.3 Warning Signs.

Buried cable warning signs or route markers are required no less than every 250 feet or at each change in route direction, both sides of street crossings, pipelines, and buried power cables.

3.2.3.4 Plow.

A cable laying plow cuts a slot as it is pulled forward. The cable is fed in and pushed to the bottom of the slot and the slot closes on it as the machine proceeds forward. Plowing should be used in range environments or other areas where there are no significant obstacles and cable runs typically exceed 1000 feet between splices.

3.2.3.5 Trench.

Trenching involves the excavation of a ditch to place the cable. To direct bury a cable, a 6-inch trench width is normally adequate. A maximum trench width of 12 inches should be utilized in direct buried applications. Hand dig at all existing manhole locations, building entrance points, utility crossings, through tree roots, under curbs, etc.

3.2.3.6 Cut/Resurface vs. Push/Bore.

See Figure 3-5: Conduit Placement and Cut & Resurface for placement details.

a. Cut and resurface should be utilized as the preferred method when crossing any paved area. Push/bore should be utilized as specified by the site DOIM for special circumstances. For road crossings on ranges, concrete encasement should be extended a minimum of 6 feet beyond the edges of the roadbed.

b. Directional boring in buried plant construction may be considered as an alternative method of installing cables or wires under highways, streets, driveways, across lawns, etc., to avoid repairing and restoring these items to their pre-construction appearances. Directional boring should be avoided for long distances in populated areas or proposed construction sites.

c. When measuring for road crossings where a push and bore may be the installation method used, ensure that there is space for the installer to place his pushing equipment and receive trench. Prior coordination should be made with the DPW to determine which roads or other surfaces cannot be cut.

d. Push and bore method should be used for railroad crossings. For railroad crossings, a minimum of a 14-inch steel casing should be used and the pipe should extend no less than 6 feet beyond each outside rail or rail bed, whichever is greater, and should be located no less than 60 inches below the base of the rails.

e. Pushes and bores should not be engineered for sites with rocky soil conditions. Cut and resurface methods should be utilized.

3.2.3.7 Depth of Placement.

According to RUS Bulletin 345-150/RUS Form 515A, the minimum depth of placement for a direct buried cable should provide cover of 24 inches in soil, 36 inches at ditch crossings and 6 inches in solid rock. To direct bury a fiber optic cable the minimum depth should provide cover of 42 inches. In solid rock, the minimum depth is reduced to 6 inches. The DOIM may have special depth requirements for certain areas (i.e., tank tracks, firing ranges, etc.).

3.2.3.8 Buried Splicing.

Buried splices should only be engineered if any of the following conditions apply: Electrical or Explosion Hazard (i.e., ammunition storage areas), Vehicular Hazard (i.e., motor pool areas), or Security Hazard (i.e., within a high security compound). All other splices in a direct buried run should be placed in pedestals or handholes and should be encapsulated. See Figure 3-7: Pedestals and Building Entrance Details for pedestal details.

3.2.4 Aerial.

Supporting documentation for aerial placement is available in RUS Bulletin 1751F-630 (http://www.usda.gov/rus/telecom/publications/1751f630.pdf) and REA TE&CM 635.

3.2.4.1 Aerial Installation Guidance.

Aerial installations should only be used in extenuating circumstances or long runs outside of the cantonment area. Small segments of aerial cable (known as "aerial inserts) may be necessary for sections of a buried cable run. The aerial inserts may span ravines, creeks or rivers, or rocky areas.

3.2.4.2 Messenger Strand.

A "2.2 M" strand should only be used as a replacement or extension of existing "2.2M" strand. A "6.6M" strand should be the smallest size strand utilized for new cable(s). Fiber optic cable should be installed on its own messenger. Copper and fiber cables should not be lashed on the same messenger. Figure-8 cable may be installed; however, no additional cable should be lashed to it.

3.2.4.3 Guys and Anchors.

Place new guys and/or anchors for each new messenger strand at each applicable location (cable turns, wind loading, cable ends, etc.). The down guy should be sized to the next larger strand.

3.2.4.4 Aerial Splices and Terminals.

a. Aerial fiber splices should not be used. The fiber optic cable should be spliced in a pedestal at the bottom of the pole.

b. Pole-mounted terminals are preferred over strand-mounted terminals.

c. Fixed-count terminals are preferred over ready-access (random-count) terminals.

d. Terminals should be placed so that no single drop exceeds 500 feet in length.

e. All terminals and splices should be supported either by attachment to the messenger cable or direct attachment to a fixed object (pole, building, pedestals, etc.). Devices should not be supported by the cable.

3.2.4.5 Horizontal Clearances for Poles/Aerial Cable.

These and additional horizontal clearances can be found in the AT&T Outside Plant Engineering Handbook (Handbook may be ordered at http://www.lucent8.com/cgi-bin/CIC_store.cgi, Document Number AT&T 900-200-318).

- Fire hydrants, signal pedestals – 4 feet
- Curbs – 6 inches
- Railroad tracks – 15 feet

- Power cables under 750 V – 5 feet or more

3.2.4.6 Vertical Clearances for Aerial Cable.

These and additional vertical clearances can be found in the AT&T Outside Plant Engineering Handbook (Handbook may be ordered at http://www.lucent8.com/cgi-bin/CIC_store.cgi, Document Number AT&T 900-200-318).

- Fire hydrants, signal pedestals – 4 feet
- Curbs – 6 inches
- Railroad tracks – 15 feet
- Power cables under 750 V – 5 feet or more

3.2.4.7 Water Protection.

Weatherproof all outdoor connections by using weather boots or other approved methods. Form a rain-drip loop at all cable entrances into buildings at points of ingress. Waterproof all building entrance points.

3.3 General Cable Specifications.

The following subparagraphs pertain to cable distances and identification:

3.3.1 Cable Distances.

Measurements between manholes from lid to lid (taken CC). Measurements from manholes to buildings, to pedestals, riser poles, etc. are from the manhole lid to the outside wall, bottom of pole, etc. (taken CP).

3.3.1.1 Buried.

Measurements for direct buried cable should be point-to-point (PP).

3.3.1.2 Aerial.

Measurements for aerial cable should be taken so that the cable could be direct buried. Measure from pole to pole and from pole to building attachments or entrance terminal etc. Do not forget to account for sag in the aerial measurements.

3.3.2 Bending Radius.

The minimum bending radius for copper cables and wires should not be less than 10 times the outside diameter of the copper cable or wire. The minimum bending radius for fiber optic cables should not be less than 20 times the outside diameter of the fiber optic cable. If cables or wires are bent too sharply, damage could occur to the copper conductors, optical fibers, shields, armors, and/or jackets of the cables or wires.

3.3.3 Cable Identification.

a. Cable tags should be installed at all termination points (terminals) and splices, including house cables. In manholes, cables should be tagged between the splice and the end wall and on both sides of a splice loop or maintenance loop. Only one tag is required for a copper cable pull-through and two tags for a fiber optic cable pull through.
b. SIZE + TYPE and CABLE ID + COUNT are required to identify copper cable.

c. Cable sizes should be identified with an abbreviation. For example, a 1200-pair cable will be identified as P12-24PF. All cables with less than 25 pairs will include an "X."

6 pair	=	P6X-24PF
12 pair	=	P12X-24PF
18 pair	=	P18X-24PF

To identify a 900 pair, 24 AWG copper cable:

P9-24PF	=	Size and Type
03, 1-900	=	Cable # and Count

(Only existing cable is identified with a 'CA' prefix.)

To identify two different cables under the same sheath:

P21-24PF
07, 1-1500+T1, 1-400+200 DD

Fiber Optic Cables should be identified with CABLE ID + COUNT and then SIZE + TYPE.

FOC 12, 1-72	=	Cable # and Strand Count
72G10F	=	Type of Cable

3.3.4 Copper.

The following paragraphs pertain to cable and reel length, cable splicing, gauge and circuit loading.

3.3.4.1 Copper Cable (Cut) Length.

To calculate the cut length of copper cable consider the following:

a. Determine the PP distance by adding together the CC distances between splice points.

b. Add 10 feet for every manhole pulled through for racking. Consider it as 5 feet extra on the cable as it comes in and 5 feet extra on the cable as it goes out.

c. For manholes with splices in them, add 20 feet to each end of the copper cable for splice length (total 40').

d. For pedestal splices add 20 feet to each cable end.

e. For cables terminating in buildings, allow for the elevation change from the trench to the PET, cable route in the building and 20 feet for the termination. If the PET is more than 50 feet inside the building, the OSP cable should be placed in EMT.

3.3.4.2 Copper Reel Length.

A list of standard copper reel lengths is included in Figure 3-2: Standard Cable Reel Lengths and Diameters. Be aware that each manufacturer may differ slightly from these numbers.

3.3.4.3 Splices.

Copper and fiber optic cable splicing shall be performed in accordance with RUS Bulletin 1735F-401, Standards for Splicing Copper and Fiber Optic Cable.

a. Self-piercing connectors should be used when splicing plastic insulated conductors. When using 25-pair splicing modules, 3M-type MS23 or equal should be used. The connectors should be consistent with previously installed connectors to preclude a requirement for a variety of installation tools by the DOIM. B-wire connectors should not be used.

b. Binder group integrity should be maintained. Split binders (of 25-pair groups) should not be spliced through any splice or taper point.

c. All dead pairs in a copper cable should be spliced through if the size of the continuing cable will allow a clear and cap at the other end. This method will provide a continuous path for the total distance of the dead pairs in case the path is needed in the future.

d. Upon completion of the splice, all underground and buried splice cases should be flash tested. After successful flash testing, the splice case should be filled with encapsulant. The splice case should be a stainless steel case or PSI Type 2. Bond cable sheaths at all cable splices with bonding harnesses to assure sheath continuity.

3.3.4.4 Cable Count Assignment.

When assigning cable counts, the center of the cable should be the last pairs assigned on a cable route. The upper or higher cable pair counts should be used first. Therefore, the highest pair count in a cable should be located closest to the switch location and the lowest pair count should be farthest away. Per the requirements of 6- and/or 12-pair terminals, pair 13 (of a binder group) rather than pair 1 is to be spared.

3.3.4.5 Cable Gauge, Resistance Design.

The preferred cable gauge is 24 AWG; however, 26 AWG may be used in high-density areas and 19 AWG may be required on longer runs (such as ranges).

To increase the signaling limit distance, start with the small gauge (large AWG number) at the dial central office and work out and up to a larger gauge (smaller AWG number), i.e., AWG 26 to AWG 24 to AWG 22 (not AWG 22 to AWG 26). Mixing gauges should be engineered in accordance with resistance charts and tables in RUS TE&CM 424 and 426.

3.3.4.6 Circuit Loading.

Analog sets/circuits should be loaded, in accordance with REA Bulletin 345-22, REA Specifications for Voice Frequency Loading, when subscriber loops extend beyond 18,000 feet.

a. When loading is required, H88 loading should be utilized: 3,000 feet from the DCO for the first load (must include calculations for tip cables, jumper wire, etc.), then every 6,000 sheath feet thereafter. End sections must be greater than 3,000 feet and less than 12,000 feet. End sections include all drops and station wire.

b. If required, build-out capacitors should be designed on trunk circuits between switches and subscriber loops for placement between load points. The build-out capacitors insert additional capacitance to compensate for distances shorter than 6000 feet between loads or between loads and end sections.

c. Pairs for any data circuit should NOT be loaded.

d. If digital or data sets (no analog) are to be used for the telephone system, NO pairs should be loaded. The user may have to provide loop extenders for long loops or the design should include pair gain devices.

3.3.5 Fiber Cabling.

All specifications for fiber optic cables should pertain to finished cable, and not raw (uncabled) fiber. The fiber optic cable should conform to the specifications contained in RUS Bulletin 1753F-601, EIA/TIA-472, and EIA 472D. All OSP fiber cable should be single-mode. Multimode fiber may be installed only in situations involving the extension of existing systems that cannot be adapted to single-mode cable.

3.3.5.1 Fiber Cable Cut Length.

To calculate the cut length of fiber optic cable consider the following:

a. The sum of the PP and/or the CC distances between splices.

b. All fiber optic cable pulled through manhole should include a 20-foot maintenance loop in addition to the 10-foot racking length.

c. In accordance with FM 11-487-5, paragraph 3-3.d, for a fiber splice in a manhole: “Assure that enough slack is pulled from both ends to have enough cable for racking and to pull 30 feet or whatever length it takes to get past the top of the manhole to the splicing trailer from each direction.”

d. Add 10 feet to each cable end for aerial splicing ends.

e. Add 65 feet to each cable end for direct buried splicing (55’ for the splice pit loop + 10’ splice end).

f. Add 20 feet for the splice end at an equipment rack location (the approximate height {2x} and width of the equipment rack).

3.3.5.2 Fiber Reel Lengths.

Fiber optic cables are available on up to 40,000-foot reels regardless of the number of strands. Small strand sizes may increase reel lengths. Actual reel lengths should be obtained from the manufacturer.

3.3.5.3 Fiber Cable Count Assignment.

Fiber optic cable strand counts should be assigned in a similar manner as copper counts. The high number counts should be dropped off first and strand one count should be the farthest from the DCO.

3.3.5.4 Use of Innerduct/Subduct.

For underground installation, each fiber optic cable should be installed in innerduct or subduct. If no innerducts are available, the installation of innerduct in the 4” conduit should be included. Fiber optic cable should not be installed directly in a 4” duct.

3.3.5.5 Splices and Power Budget.

In accordance with RUS Bulletin 1751F-642 (http://www.usda.gov/rus/telecom/publications/1751f642.pdf), for buried fiber optic cable plant, direct buried filled splice cases installed in manholes and handholes are preferred over burying the splice.

4.□.□.□ Every effort should be made to utilize “loop through” splicing in lieu of homeruns/dedicated cables to the serving location. In “loop through” splicing, only the fiber strands breaking off from the main cable are cut and spliced. The other fibers are not cut. The sheath is cut from the cable, the exiting fibers cut and spliced, and the remaining fibers are simply folded back within the case (not cut) and then routed on.

The power budget should be calculated for the fiber optic cable run. If the loss is too great for a standard laser, a long-range laser should be considered.

3.4 Sizing Requirements.

The following information pertains to copper and fiber optic sizing requirements between the MCN to Alternate Main Communications Node (A-MCN), MCN to ADN and ADN to EUB.

3.4.1 Copper.

The number of OSP copper pairs is calculated by multiplying the number of users or jumpers in the building times 1.5 pairs. This factor will add in some additional pairs for faxes, modems, and special circuits. The cable is then sized to the nearest logical standard cable size. For example, a building with 85 users would require a 200-pair cable (85 x 1.5 = 128 ➔ 200 pair).

3.4.2 Fiber.

Fiber optic cable should be used for MCN to A-MCN, MCN to ADN, and ADN to EUB cable runs.

3.4.2.1 MCN to Alternate Main Communications Node (A-MCN).

For planning purposes, use a minimum of 48 strands between the MCN and the A-MCN to provide load balancing and network reliability. Only the strands destined for that MCN/A-MCN should be routed into the building.

3.4.2.2 MCN to ADN.

A minimum of 24 strands of single-mode fiber optic cable should be installed between the ADN/MCNs. Some of these 24 strands should be used to provide logical connectivity to two adjacent ADNs. In accordance with Paragraph 2.3.5.6.6, splices for physical route diversity and connection to adjacent ADNs should be done in the manhole outside the MCN/ADN. Only strands destined for that MCN/ADN should be routed into the building. For ADN locations containing more than 2 ADN chassis, additional fibers should be installed. An additional 24 strands should be installed for each 2 chassis (for example, 3 or 4 chassis, install 48 strands).

3.4.2.3 ADN to EUB.

A minimum of 12 strands of fiber should be installed to connect the ADNs to the EUBs. If multiple edge devices are required in an EUB, a minimum of 24 strands of fiber should be installed. The number of edge devices used in a building is based on distance to user (Ethernet distance limit 295 ft), numbers of users in the building, and the bandwidth requirements. See .

3.4.3 Physical Route Diversity and Concrete-Encasement.

If it is not economically feasible to create physically diverse links between the MCNs/ADNs, concrete-encased duct should be used to minimize the impact of damage due to digging or natural catastrophe. All dual-homed buildings (MCNs, ADNs, and critical EUBs) that have only one entry point should have concrete-encased duct to the nearest manhole.

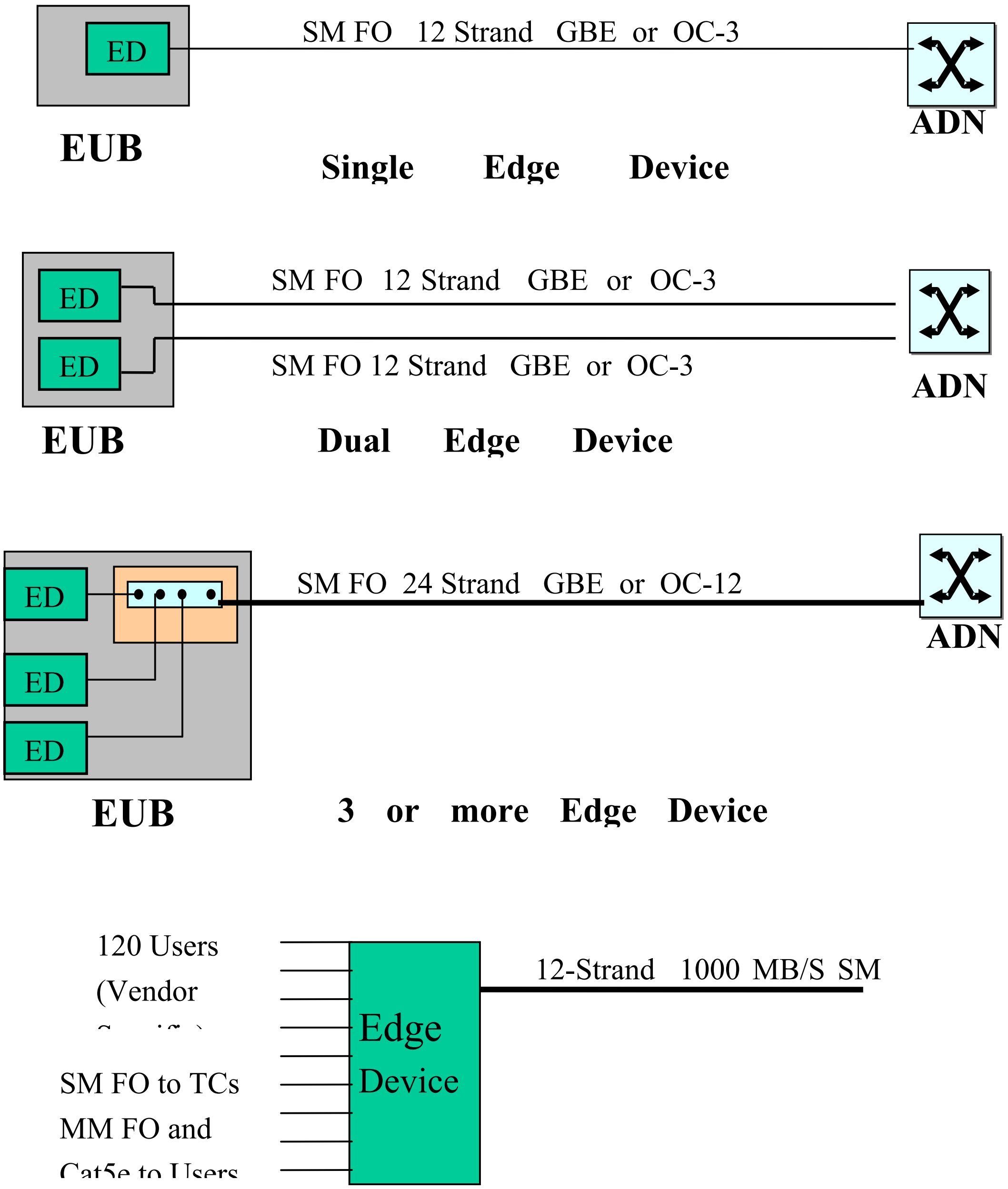


Figure 3-1: Typical EUB Configurations

	Number of Pairs	AWG	Standard Length (ft)	Nominal Diameter (in)
	6X	19	5000	0.53
PE-22	12X	19	5000	0.6
Air Core	25	19	5000	0.81
Alpeth	50	19	2500	1.08
Sheath	6X	22	5000	0.43
	12X	22	5000	0.53
	25	22	5000	0.7
	50	22	5000	0.85
	100	22	5000	1.07
	200	22	5000	1.48
	300	22	2000	1.75
	400	22	2000	1.96
	600	22	1000	2.44
	900	22	1000	2.88
	1200	22	750	3.29
	6X	24	10000	0.41
	12X	24	10000	0.46
	25	24	10000	0.55
	50	24	5000	0.66
	100	24	5000	0.87
	200	24	5000	1.18
	300	24	2500	1.38
	400	24	2500	1.53
	600	24	2500	1.85
	900	24	1500	2.31
	1200	24	1000	2.69
	1500	24	1000	2.92
	1800	24	750	3.01
	2100	24	500	3.39

Figure 3-2: Standard Cable Reel Lengths and Diameters

	Number of Pairs	AWG	Standard Length (ft)	Nominal Diameter (in)
	25	26	10000	0.49
	50	26	10000	0.57
	100	26	10000	0.71
	200	26	5000	0.97
	300	26	5000	1.14
	400	26	5000	1.30
	600	26	2500	1.54
	900	26	2500	1.88
	1200	26	1500	2.10
	1500	26	1500	2.32
	1800	26	1000	2.48
	2100	26	1000	2.68
	2400	26	1000	2.90
	2700	26	1000	3.03
	3000	26	750	3.20

	Number of Pairs	AWG	Standard Length (ft)	Nominal Diameter (in)
	6X	22	9930	0.96
Figure-8	12X	22	9930	1
Filled	25	22	9810	1.16
Self-Supported	50	22	6540	1.34
Alpeth	6X	24	11340	0.88
Sheath	12X	24	11340	0.96

	Number of Pairs	AWG	Standard Length (ft)	Nominal Diameter (in)
	25	24	11340	1.02
	50	24	11340	1.18
	50	26	13320	1.08
	100	26	8820	1.26

	Number of Pairs	AWG	Standard Length (ft)	Nominal Diameter (in)
	6X	19	5000	0.52
PE-89	12X	19	5000	0.62
Filled	25	19	5000	0.86
Alpeth	50	19	5000	1.12
Sheath	100	19	2500	1.51
	200	19	1500	2.04
	6X	22	5000	0.48
	12X	22	5000	0.52
	25	22	5000	0.66
	50	22	5000	0.86
	75	22	5000	0.96
	100	22	5000	1.1
	150	22	5000	1.32
	200	22	2500	1.49
	300	22	2000	1.72
	400	22	2000	1.96
	600	22	1000	2.4
	900	22	1000	2.9
	1200	22	750	3.28
	6X	24	10000	0.44
	12X	24	10000	0.48
	25	24	10000	0.58
	50	24	10000	0.7
	75	24	5000	0.86
	100	24	5000	0.94
	150	24	5000	1.06
	200	24	5000	1.2
	300	24	2500	1.45

Figure 3-2 (cont.): Standard Cable Reel Lengths and Diameters

	Number of Pairs	AWG	Standard Length (ft)	Nominal Diameter (in)
	400	24	2000	1.59
	600	24	2000	1.92
	900	24	1000	2.32
	1200	24	1000	2.68
	1500	24	1000	2.92
	1800	24	750	3.2
	2100	24	600	3.44
	25	26	10000	0.52
	50	26	10000	0.58
	100	26	10000	0.78
	200	26	5000	1.02
	300	26	5000	1.18
	400	26	5000	1.33
	600	26	2500	1.59
	900	26	2000	1.92
	1200	26	1500	2.1
	1500	26	1000	2.34
	1800	26	1000	2.6
	2100	26	1000	2.78
	2400	26	1000	2.92
	2700	26	750	3.14
	3000	26	750	3.24

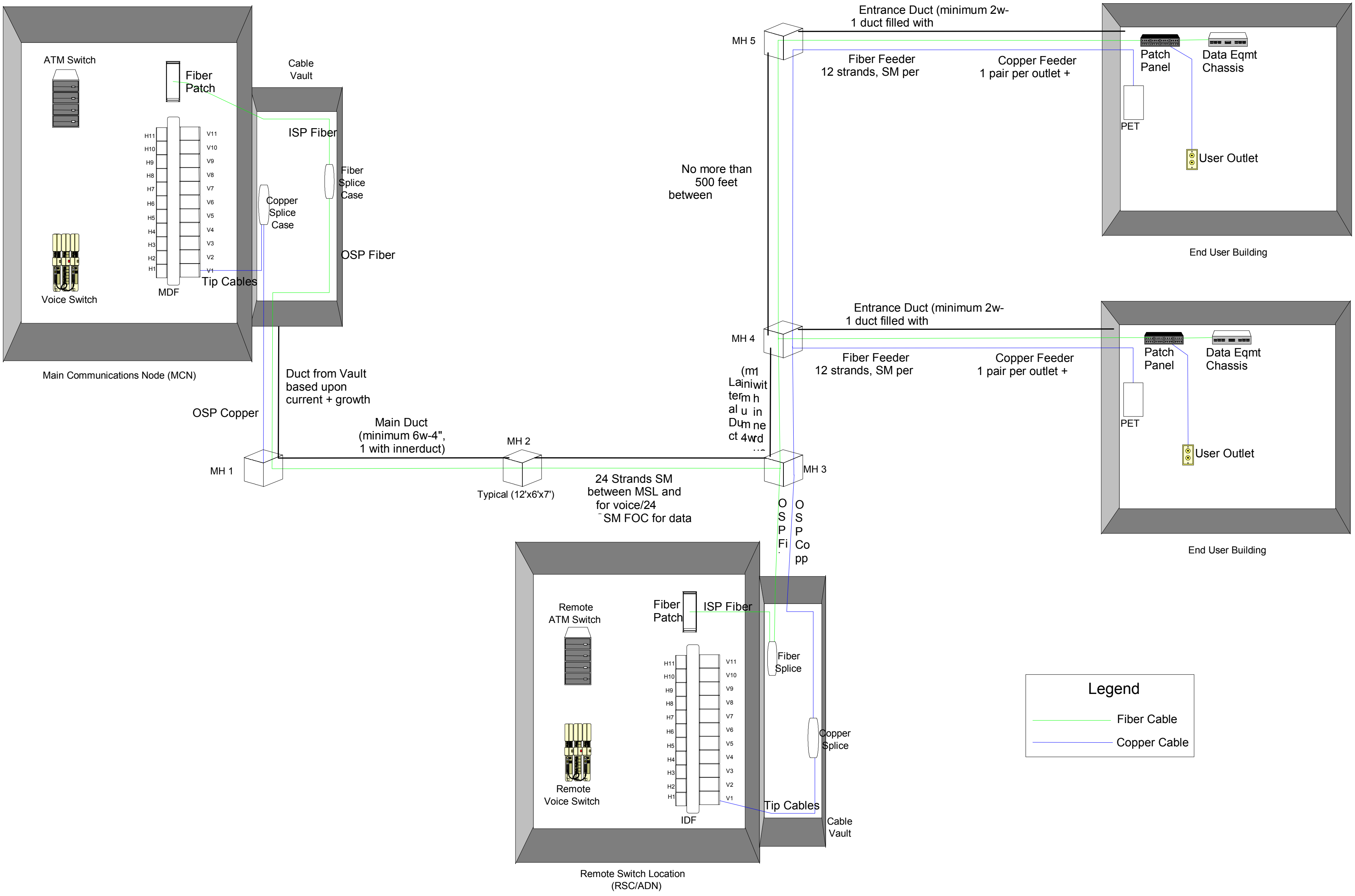
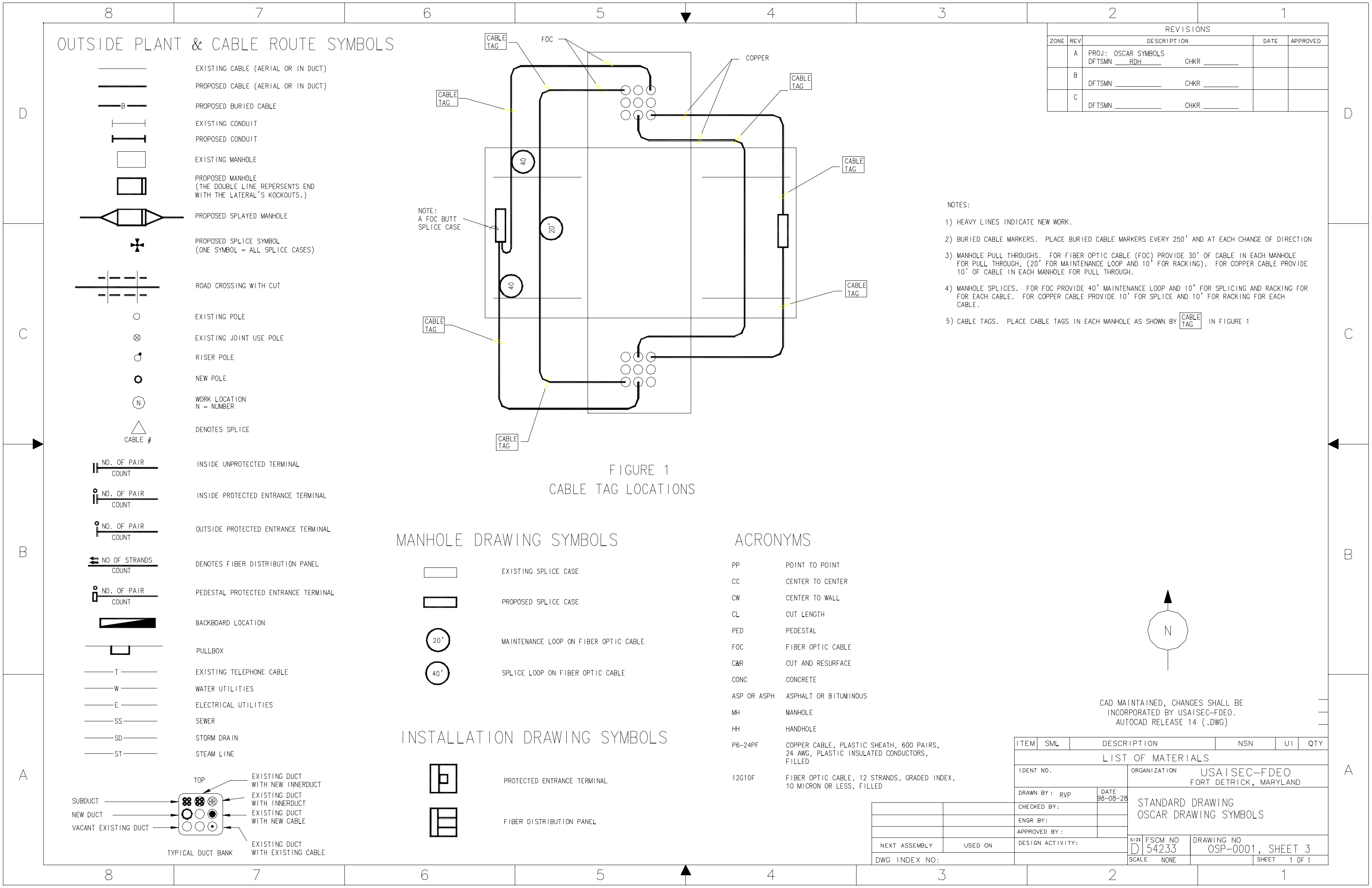


Figure 3-3: OSP Infrastructure Standard



REVISIONS

ZONE	REV	DESCRIPTION	DATE	APPROVED
	A	PROJ: OSCAR SYMBOLS DFTSMN RDH CHKR		
	B	DFTSMN CHKR		
	C	DFTSMN CHKR		

NOTES:

1) HEAVY LINES INDICATE NEW WORK.

2) BURIED CABLE MARKERS. PLACE BURIED CABLE MARKERS EVERY 250' AND AT EACH CHANGE OF DIRECTION

3) MANHOLE PULL THROUGHS. FOR FIBER OPTIC CABLE (FOC) PROVIDE 30' OF CABLE IN EACH MANHOLE FOR PULL THROUGH, (20' FOR MAINTENANCE LOOP AND 10' FOR RACKING). FOR COPPER CABLE PROVIDE 10' OF CABLE IN EACH MANHOLE FOR PULL THROUGH.

4) MANHOLE SPLICES. FOR FOC PROVIDE 40' MAINTENANCE LOOP AND 10' FOR SPLICING AND RACKING FOR FOR EACH CABLE. FOR COPPER CABLE PROVIDE 10' FOR SPLICE AND 10' FOR RACKING FOR EACH CABLE.

5) CABLE TAGS. PLACE CABLE TAGS IN EACH MANHOLE AS SHOWN BY CABLE TAG IN FIGURE 1

ACRONYMS

PP	POINT TO POINT
CC	CENTER TO CENTER
CW	CENTER TO WALL
CL	CUT LENGTH
PED	PEDESTAL
FOC	FIBER OPTIC CABLE
C&R	CUT AND RESURFACE
CONC	CONCRETE
ASP OR ASPH	ASPHALT OR BITUMINOUS
MH	MANHOLE
HH	HANDHOLE
P6-24PF	COPPER CABLE, PLASTIC SHEATH, 600 PAIRS, 24 AWG, PLASTIC INSULATED CONDUCTORS, FILLED
12G10F	FIBER OPTIC CABLE, 12 STRANDS, GRADED INDEX, 10 MICRON OR LESS, FILLED

CAD MAINTAINED, CHANGES SHALL BE
INCORPORATED BY USAISEC-FDEO.
AUTOCAD RELEASE 14 (.DWG)

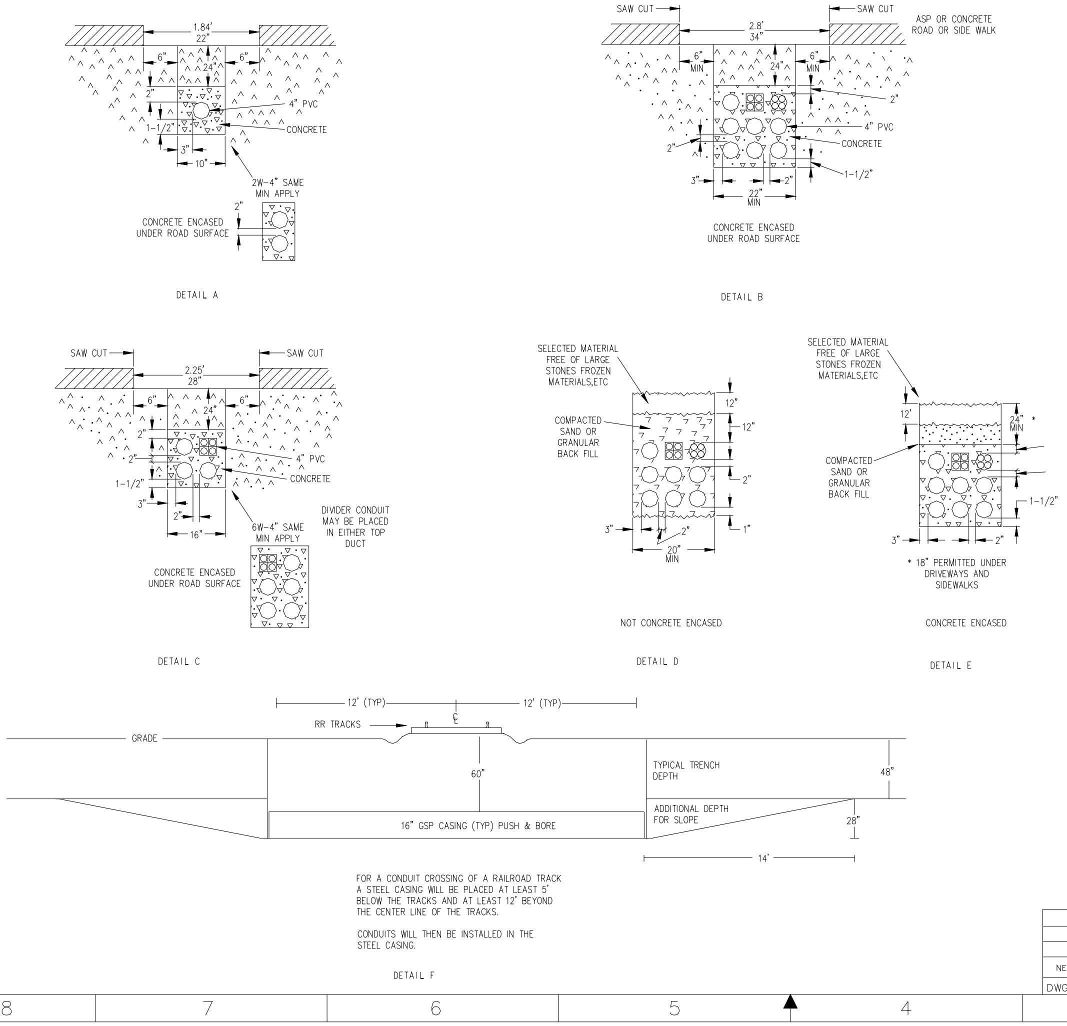
ITEM	SML	DESCRIPTION	NSN	UI	QTY

LIST OF MATERIALS

IDENT NO.		ORGANIZATION	USAISEC-FDEO FORT DETRICK, MARYLAND
DRAWN BY: RVP	DATE 98-08-28	STANDARD DRAWING OSCAR DRAWING SYMBOLS	
CHECKED BY:			
ENGR BY:			
APPROVED BY:			
DESIGN ACTIVITY:		SIZE D FSCM NO 54233	DRAWING NO OSP-0001, SHEET 3
		SCALE NONE	SHEET 1 OF 1

NEXT ASSEMBLY	USED ON
DWG INDEX NO:	

Figure 3-4: Drawing Symbols


SAW CUT
SAW CUT
ASP OR CONCRETE ROAD OR SIDE WALK
1.84'
22"
6"
24"
6"
2"
4" PVC
1-1/2"
CONCRETE
3"
10"
2W-4" SAME MIN APPLY
2"
CONCRETE ENCASED UNDER ROAD SURFACE
DETAIL A
2.8'
34"
6" MIN
24"
6" MIN
2"
4" PVC
2"
CONCRETE
1-1/2"
3"
2"
22" MIN
CONCRETE ENCASED UNDER ROAD SURFACE
DETAIL B
2.25'
28"
6"
24"
6"
2"
2"
4" PVC
CONCRETE
1-1/2"
3"
2"
16"
6W-4" SAME MIN APPLY
DIVIDER CONDUIT MAY BE PLACED IN EITHER TOP DUCT
CONCRETE ENCASED UNDER ROAD SURFACE
DETAIL C
SELECTED MATERIAL FREE OF LARGE STONES FROZEN MATERIALS,ETC
COMPACTED SAND OR GRANULAR BACK FILL
12"
12"
2"
1"
3"
2"
20" MIN
NOT CONCRETE ENCASED
DETAIL D
SELECTED MATERIAL FREE OF LARGE STONES FROZEN MATERIALS,ETC
12'
24" MIN *
COMPACTED SAND OR GRANULAR BACK FILL
1-1/2"
3"
2"
* 18" PERMITTED UNDER DRIVEWAYS AND SIDEWALKS
CONCRETE ENCASED
DETAIL E
12' (TYP)
12' (TYP)
℄
RR TRACKS
GRADE
60"
TYPICAL TRENCH DEPTH
48"
16" GSP CASING (TYP) PUSH & BORE
ADDITIONAL DEPTH FOR SLOPE
28"
14'

FOR A CONDUIT CROSSING OF A RAILROAD TRACK A STEEL CASING WILL BE PLACED AT LEAST 5' BELOW THE TRACKS AND AT LEAST 12' BEYOND THE CENTER LINE OF THE TRACKS.

CONDUITS WILL THEN BE INSTALLED IN THE STEEL CASING.

DETAIL F

REVISIONS

ZONE	REV	DESCRIPTION	DATE	APPROVED
	A	PROJ: OSCAR SYMBOLS DFTSMN RDH CHKR ________		
	B	DFTSMN ________ CHKR ________		
	C	DFTSMN ________ CHKR ________		

NOTES:

1. CONTRACTOR SHALL FURNISH AND INSTALL CONDUITS.
2. CONDUIT FORMATIONS SHOULD PERMIT STANDARD CABLE RACKING WITHOUT CHANGING THE CONDUIT FORMATION AS IT ENTERS THE MANHOLE. IF THE TOTAL NUMBER OF DUCTS IS SIGNIFICANTLY LESS THAN THE CAPACITY OF THE MANHOLE, THE DUCTS SHOULD ENTER IN THE LOWER PORTION OF THE KNOCKOUT SLOT TO SIMPLIFY FUTURE CONDUIT ADDITIONS.
3. THE TRENCH FOR MULTIPLE CONDUIT DUCT SHOULD BE NO GREATER THAN NEEDED TO PROVIDE ADEQUATE WORKING SPACE. FOR SINGLE DUCT (UNENCASED OR ENCASED) THE TRENCH SHOULD BE THE WIDTH OF THE DUCT STRUCTURE PLUS 3 INCHES (5CM) ON EACH SIDE. ALL CONDUIT THAT IS TO BE ENCASED IN CONCRETE SHOULD HAVE APPROXIMATELY 1.5 INCHES (3.81CM) OF CLEARANCE BETWEEN BOTTOM ROW OF DUCTS AND THE TRENCH BOTTOM.
4. SUBJECT TO FEDERAL, STATE AND LOCAL REQUIREMENTS. THE DEPTH OF THE TRENCH SHOULD BE AT LEAST THE HEIGHT OF THE CONDUIT STRUCTURE PLUS 23.5 INCHES (59.69CM). A MINIMUM OF 18 INCHES (46.72CM) IS SUFFICIENT WHEN CONDUIT IS PLACED UNDER DRIVEWAYS, SIDEWALKS AND OFF THE TRAVELED PART OF THE RIGHT-OF-WAY.
5. THE CONTRACTOR SHALL ESTABLISH FINAL GRADES WITH THE FACILITY ENGINEERS BEFORE EXCAVATING FOR ANY PROPOSED CONDUIT RUNS.
6. ALL NEWLY INSTALLED CONDUITS SHALL BE ROD & MANDRELLED. PULL WIRES SHALL BE PROVIDED IN ALL NEWLY INSTALLED CONDUITS.
7. THE CONTRACTOR SHALL COORDINATE ALL ROAD BORING WITH THE FACILITIES ENGINEER AND MEET THE FACILITIES ENGINEERS REQUIREMENTS FOR RIGHT-OF-WAY AND DEPTH OF COVER.
8. THE CONTRACTOR SHALL COORDINATE THE PLACEMENT OF ATTACHING CONDUITS TO EXISTING BRIDGES.
9. THE CONTRACTOR SHALL ADHERE TO RUS BULLETIN 1751F-643 FOR ALL CONDUIT PLACING AND BENDING RADIUS.
10. THE LARGEST DIAMETER COPPER CABLES SHOULD BE PLACED IN THE LOWEST VACANT DUCT.
11. SUB-DUCT, INNERDUCT AND FIBER OPTIC CABLES SHOULD BE PLACED IN THE UPPER EMPTY DUCTS.

CAD MAINTAINED, CHANGES SHALL BE
INCORPORATED BY USAISEC-FDEO.
AUTOCAD RELEASE 14 (.DWG)

ITEM	SML	DESCRIPTION	NSN	UI	QTY

LIST OF MATERIALS

IDENT NO.

ORGANIZATION USAISEC-FDEO
FORT DETRICK, MARYLAND

DRAWN BY: SAIC DATE 98-08-28

CHECKED BY:

ENGR BY:

APPROVED BY:

DESIGN ACTIVITY:

NEXT ASSEMBLY USED ON

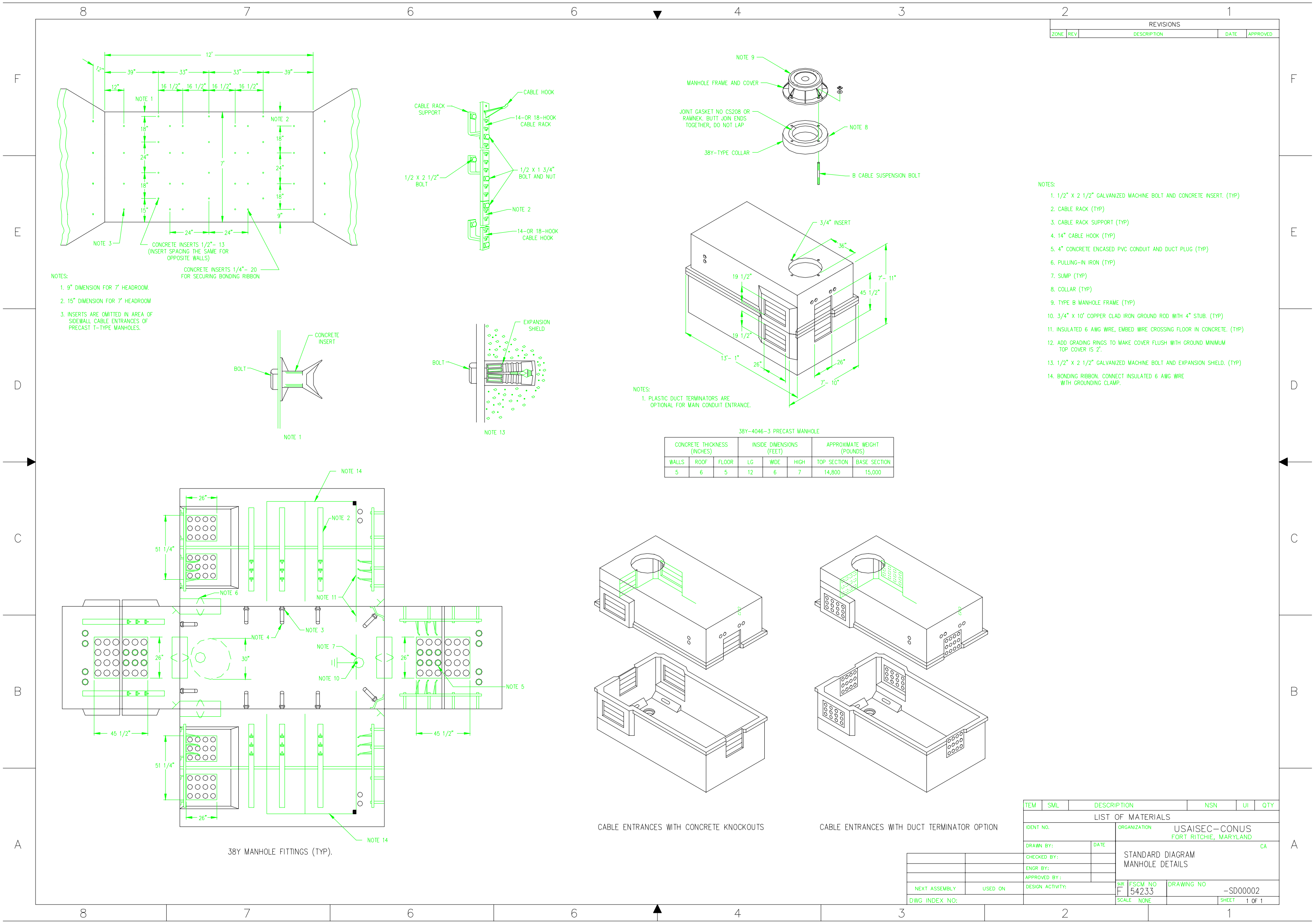
DWG INDEX NO:

STANDARD DIAGRAM
CONDUIT PLACEMENT &
CUT & RESURFACE DETAILS

SIZE D FSCM NO 54233 DRAWING NO OSP-0001, SHEET 4

SCALE NONE SHEET 1 OF 1

Figure 3-5: Conduit Placement and Cut & Resurface



REVISIONS

ZONE	REV	DESCRIPTION	DATE	APPROVED

NOTES:

1. 9" DIMENSION FOR 7' HEADROOM.
2. 15" DIMENSION FOR 7' HEADROOM
3. INSERTS ARE OMITTED IN AREA OF SIDEWALL CABLE ENTRANCES OF PRECAST T-TYPE MANHOLES.

NOTES:

1. PLASTIC DUCT TERMINATORS ARE OPTIONAL FOR MAIN CONDUIT ENTRANCE.

38Y-4046-3 PRECAST MANHOLE

CONCRETE THICKNESS (INCHES)			INSIDE DIMENSIONS (FEET)			APPROXIMATE WEIGHT (POUNDS)	
WALLS	ROOF	FLOOR	LG	WIDE	HIGH	TOP SECTION	BASE SECTION
5	6	5	12	6	7	14,800	15,000

NOTES:

1. 1/2" X 2 1/2" GALVANIZED MACHINE BOLT AND CONCRETE INSERT. (TYP)
2. CABLE RACK (TYP)
3. CABLE RACK SUPPORT (TYP)
4. 14" CABLE HOOK (TYP)
5. 4" CONCRETE ENCASED PVC CONDUIT AND DUCT PLUG (TYP)
6. PULLING-IN IRON (TYP)
7. SUMP (TYP)
8. COLLAR (TYP)
9. TYPE B MANHOLE FRAME (TYP)
10. 3/4" X 10' COPPER CLAD IRON GROUND ROD WITH 4" STUB. (TYP)
11. INSULATED 6 AWG WIRE, EMBED WIRE CROSSING FLOOR IN CONCRETE. (TYP)
12. ADD GRADING RINGS TO MAKE COVER FLUSH WITH GROUND MINIMUM TOP COVER IS 2'.
13. 1/2" X 2 1/2" GALVANIZED MACHINE BOLT AND EXPANSION SHIELD. (TYP)
14. BONDING RIBBON. CONNECT INSULATED 6 AWG WIRE WITH GROUNDING CLAMP.

ITEM	SML	DESCRIPTION	NSN	UI	QTY

LIST OF MATERIALS

IDENT NO.

ORGANIZATION USAISEC–CONUS
FORT RITCHIE, MARYLAND

DRAWN BY: | DATE
CHECKED BY:
ENGR BY:
APPROVED BY:
DESIGN ACTIVITY:

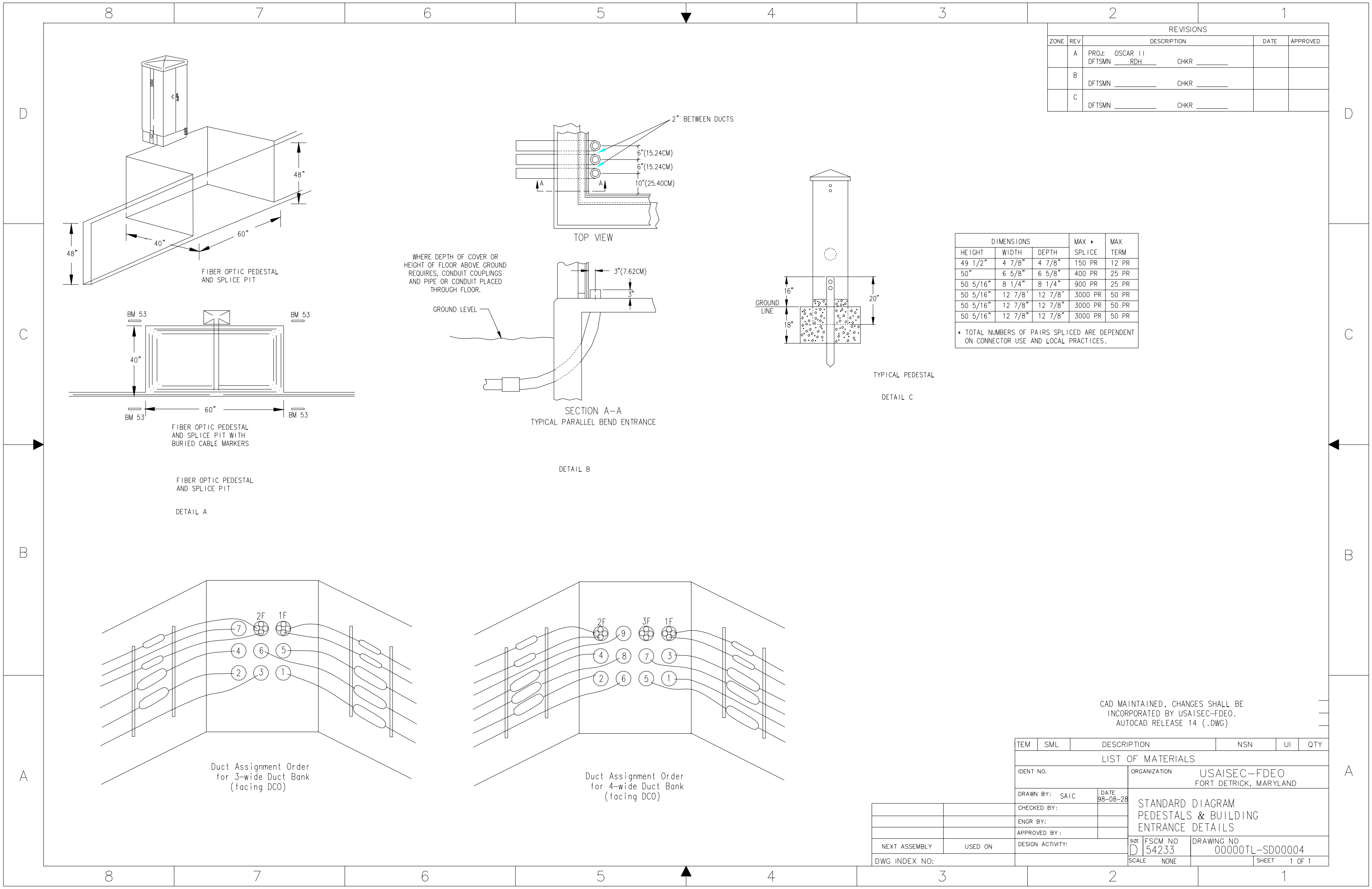
CA

STANDARD DIAGRAM
MANHOLE DETAILS

NEXT ASSEMBLY | USED ON
DWG INDEX NO:

SIZE F | FSCM NO 54233 | DRAWING NO –SD00002
SCALE NONE | SHEET 1 OF 1

Figure 3-6: Manhole Typical



REVISIONS				
ZONE	REV	DESCRIPTION	DATE	APPROVED
	A	PROJ: OSCAR II DFTSMN ___RDH___ CHKR ________		
	B	DFTSMN __________ CHKR ________		
	C	DFTSMN __________ CHKR ________		

DIMENSIONS			MAX *	MAX
HEIGHT	WIDTH	DEPTH	SPLICE	TERM
49 1/2"	4 7/8"	4 7/8"	150 PR	12 PR
50"	6 5/8"	6 5/8"	400 PR	25 PR
50 5/16"	8 1/4"	8 1/4"	900 PR	25 PR
50 5/16"	12 7/8'	12 7/8'	3000 PR	50 PR
50 5/16"	12 7/8"	12 7/8"	3000 PR	50 PR
50 5/16"	12 7/8"	12 7/8"	3000 PR	50 PR

* TOTAL NUMBERS OF PAIRS SPLICED ARE DEPENDENT ON CONNECTOR USE AND LOCAL PRACTICES.

Figure 3-7: Pedestals and Building Entrance Details

4.0 DIAL CENTRAL OFFICE / REMOTE SWITCHING UNIT .

4.1 Dial Central Office Specifications.

Most of the information in this section was imported from Automated Information System (AIS) Design Guidance, Telephone Systems developed by United States Army Information Systems Engineering Command (USAISEC), October 1999 (http://www.isec-sig.army.mil/ISECTech/Guides/telesys/telesystg.htm). If accessing from a ".mil" location a log-on and password is not required. If accessing from an address other than ".mil" click on the following site to obtain a log-on and password (ensure to include the organization that you represent and that it's for the I3A Implementation Guide). (http://www.isec-sig.army.mil/isectech/help.htm).

4.2 Switch Location and Layout.

An example of a Dial Central Office (DCO) switch room is included in Figure 4-2: Typical Switch Room Layout.

4.3 Site Preparation Design Parameters.

The following paragraphs list generic floor space, power, heating, ventilation, and air-conditioning parameters that can be used when planning DCO or Remote Switching Unit (RSU) system installations. The manufacturer specifications should be followed for the exact model of equipment being installed. The tables are based on the expansion size of the switch.

4.3.1 DCO Floor Space and Heat Loads.

DCO Air Conditioning Calculations:							
DCO SIZE	Room Size	Switch	Ambient	Lights	Total	Convert to Tons	Required
(Lines)	Square ft	BTU/hr	BTU/hr	BTU/hr	BTU/hr	Tons/12,000BTU	Tons
1920 to 2880	600	54,608	15,000	6,145	75,753	6.3	7.5
2880 to 3840	800	72,810	20,000	8,191	101,002	8.4	10
3840 to 4800	1,000	91,013	25,000	10,239	126,252	10.5	12
4800 to 5760	1,500	109,216	37,500	15,360	162,076	13.5	15
5760 to 6720	1,750	127,420	43,750	17,918	189,088	15.75	20
6720 to 7680	1,750	145,621	43,750	17,918	207,289	17.3	20
7680 to 8640	1,750	163,824	50,000	20,478	234,302	19.5	20
8640 to 9600	2,000	182,026	50,000	20,478	252,504	21	24
9600 to 10,560	2,000	200,229	50,000	20,478	270,707	22.5	24
10,560 to 11,520	2,500	218,432	62,500	25,600	306,532	25.5	30
11,520 to 12,480	2,500	236,635	62,500	25,600	324,735	27	30
12,480 to 13,440	2,500	254,837	62,500	25,600	342,937	28.5	30
13,440 to 14,400	2,750	273,040	68,750	28,157	369,947	30.8	36
14,400 to 15,360	2,750	291,243	68,750	28,157	388,150	32.5	36
15,360 and above	3,000	300,000	75,000	30,717	405,717	34	36

4.3.2 DCO Electrical Loads.

DCO Electrical Load Calculations:							
DCO SIZE (Lines)	Switch Load KW	Air Cond Load KW	Lights KW	Total KW	Growth Factor 1.25xKW	Generator Size KW	Transformer Size KVA
1920 to 2880	21	22.5	1.8	45.3	56.6	60	75
2880 to 3840	28	30	2.4	60.4	75	75	100
3840 to 4800	35	36	3	74	92.5	100	125
4800 to 5760	42	45	4.5	91.5	114.5	125	150
5760 to 6720	49	60	5.25	114.25	143	150	200
6720 to 7680	56	60	5.25	121.25	151	150	200
7680 to 8640	63	60	6	129	161	180	225
8640 to 9600	70	72	6	148	185	200	250
9600 to 10,560	77	72	6	155	193.75	200	250
10,560 to 11,520	85	90	7.5	182.5	228	250	300
11,520 to 12,480	92	90	7.5	189.5	237	250	300
12,480 to 13,440	99	90	7.5	196.5	245.5	250	300
13,440 to 14,400	106	108	8.25	222.25	278	300	400
14,400 to 15,360	113	108	8.25	229.25	286.5	300	400
15,360 and above	120	108	9	237	296.5	350	500

4.3.3 RSU Floor Space and Electrical Loads.

Electrical Load Calculations: Remote Switch Units								
RSU SIZE (Lines)	Room Size Sq ft	AC Load KW	Switch Load KW	Lights KW	Recept KW	Total KW	Growth Factor 1.25xKW	Recommended Generator Size KW
0 to 960	225	9	7	0.72	0.7	17.42	21.78	25
960 to 1920	350	9	14	1.12	1.05	25.17	31.46	50
1920 to 2880	500	15	21	1.6	1.5	39.1	48.88	50
2880 to 3840	600	15	28	1.92	1.8	46.72	58.4	60
3480 to 4800	800	18	35	2.56	2.4	57.96	72.45	80
4800 to 5760	1000	22.5	42	3.2	3	70.7	88.38	100
5760 to 6500	1200	22.5	49	3.84	3.6	78.94	98.67	100
6500 and up	over 1200	30	56	4.8	4.5	95.3	119.12	125

4.3.4 RSU Heat Loads.

Air Conditioning Load Calculations: Remote Switch Units									
RSU SIZE (Lines)	Line Cabinets	BTU/hr	Control Cabinets	BTU/hr	Rectifier BTU/hr	Misc BTU/hr	Total BTU/hr	Total Tons	Recommended AC Size Tons
0 to 960	1	3,547	1	4,433	5,184	6,468	19,632	1.64	3 Tons
960 to 1920	2	7,094	1	4,433	5,184	6,468	23,179	1.93	3 Tons
1920 to 2880	3	10,641	2	8,866	7,776	11,788	39,071	3.26	3 up to 5 tons
2880 to 3840	4	14,188	2	8,866	10,600	11,788	45,442	3.79	5 Tons
3480 to 4800	5	17,735	3	13,299	13,192	14,448	58,674	4.89	5 up to 6 tons
4800 to 5760	6	21,282	3	13,299	16,016	17,108	67,705	5.64	6 up to 7.5 tons
5760 to 6720	7	24,829	4	17,732	18,840	17,108	78,509	6.54	7.5 Tons

4.3.5 Batteries.

The batteries should be sized to support the expansion size of the switch. RUS Bulletin 1751E-302), Power Requirements for Digital Central Office Equipment, (http://www.usda.gov/rus/telephone/regs/1751e302.htm) also recommends the battery provided should have the capacity to maintain the central office load for a period of 8 hours. It also states that systems equipped with emergency generators are allowed to reduce the 8 hours to a 3-hour reserve time.

4.3.6 Generator.

The fuel tank should be sized for 2 days of operation. Other supporting design parameters can be found in RUS Bulletin 1751E-320, Emergency Generating and Charging Equipment (http://www.usda.gov/rus/telephone/regs/1751e320.htm).

4.3.7 Main Distribution Frame.

The main distribution frame (MDF) is the interface between the OSP cable and the switch cables. The iron framework of the MDF supports the horizontal blocks and vertical connectors. If new vertical sections are required, a minimum of 30 inches of clearance is required for safety.

4.3.7.1 Horizontal Blocks.

The horizontal blocks terminate the tie cables between the switch and the MDF. Each connection corresponds to a telephone number on the switch. The switch contractor determines the number of horizontal blocks on the frame. All horizontals should be stenciled to show the termination identifications.

4.3.7.2 Vertical Connectors.

The vertical connectors are mounted on the vertical side of the MDF. Each connector protects 100 pairs of the OSP cables. The connector is equipped with tip cables that are pre-terminated on the connector. The tip cables are routed from the MDF, through the floor, to the cable vault and are spliced to the OSP cable. The vertical connectors protect the electronics in the DCO by providing lightning and surge protection. Each termination corresponds to a pair of the OSP. All OSP pairs should be terminated on connectors. All verticals should be stenciled to show the cable number and the pair count for all connectors on that vertical. All connectors should show the count terminated.

a. No more than six MDF connectors should be designed for frames less than 9 feet high.

b. No more than eight MDF connectors should be designed for frames 9 feet high.

c. A schematic showing the vertical side of the MDF is included in Figure 4-1: MDF and Cable Vault Schematic.

4.3.7.3 Cross Connects.

Cross connects are installed between the OSP terminations on the vertical connectors and the switch terminations on the horizontal blocks. This process connects an OSP pair to a telephone number. Approximately 8 inches of slack should be left in the cross connect wire to allow re-termination for moves, adds, or changes.

4.3.7.4 Special Circuits.

Since special circuits (such as data circuits, T1s, or alarms) are usually non-switched, they should be treated differently than voice and modem circuits. The protector modules should be marked to indicate a special circuit. Various colors of protector modules are available to help in this differentiation. The special circuits should be cross connected to designated blocks on the horizontal side (not to the switch blocks).

4.3.7.5 Grounding.

Schematics showing the details of voice switch grounding are included in Figure 4-3: Grounding Schenmatic.

2.3.5.6.11 4.3.7.5.1 Maximum Impedance.

Most manufacturers require impedance from the ground ring to earth potential of ≤ 5 ohms. Impedance measurements should be made using a direct reading ground resistance meter.

a. Since the telephone system is usually installed by a commercial contractor and is warranted by that contractor, the system should be grounded in accordance with the manufacturer's practices. However, the manufacturer's practices, as shown on the construction drawings, should be reviewed for compliance with the following recommendations:

b. The components of a typical telephone central office grounding system are shown in Figure 4-3: Grounding Schematic, and include the following:

1. An earth electrode system, which consists of, ground rods driven into the earth around the perimeter of the switch building or in a triangular pattern in an open area just outside the switch room. These rods are exothermically bonded with a bare power wire (minimum size of 1/0 AWG). This system is commonly called the "ground ring".

2. The master ground bar (MGB) is usually mounted in the switch room on an outside wall and is the tie point for the ironwork, cabinet grounds, floor tile, and the reference ground for the -48V battery power plant. It is connected to the ground ring with an insulated wire, which is sized to meet the requirements of the National Electrical Code (NEC). NEC Ordering information available at http://catalog.nfpa.org/ - 1. This system is the "single point ground" of the central office grounding scheme.

3. The cable entrance ground bar (CEGB) is a tie point in the cable vault or cable entrance area which facilitates bonding of the OSP cable sheaths directly to the ground ring.

4. The MDF ground bar is a tie point for cable pair protection and is usually isolated from the MDF ironwork. The MDF ground bar is usually connected to the MGB with an insulated (minimum #6 AWG) wire.

5. The power distribution board is the cabinet or frame, which contains fuses (or direct current (DC) circuit breakers) for the distribution of -48V DC circuits. Its ground bar serves as a tie point for all circuit returns and the power wires to the positive side of the battery string. This ground bar is also connected to the MGB.

6. The battery string is a group of individual cells strapped in an amount and with a configuration which should meet the ampere-hour requirements of the specification. The direct current is filtered by the battery string, which also provides no-break power to the switch. The positive side of the string is connected to the power distribution board ground bar.

7. The rectifiers, sometimes called “chargers,” convert 208V AC (commercial power) to -48V DC. The positive side of the rectifier outputs connects to the power distribution board ground bar, thus is in parallel to the battery string.

4.3.8 Cable Vault Guidance.

Figure 4-1: MDF and Cable Vault Schematic is a schematic of an MDF and cable vault.

a. The cable vault should extend the entire length of the MDF.

b. A center rack is preferable for the splicing of the tip cables to the OSP cables. However, wall racking is allowable for small to medium central offices. The vault should be designed to allow ample space for splicing of the cables. For planning, a typical vault splice is 1 foot x 3 feet.

4.4 Voice Switch.

The following paragraphs describe voice switching terminology.

a. Installed Size - The total number of lines needed to support user and non-user voice outlets requiring dial tone and a unique telephone number. Installed size accounts for user population at time of startup or cutover.

b. Equipped Size - The total number of lines available on the installed backplane for user and non-user voice outlets when the switch is operating at its maximum installed capacity. Additional line cards may be required to reach this level. The equipped size provides for anticipated user population growth.

c. Expandable Size - The total number of lines available for user and non-user voice outlets when the switch is expanded to its maximum design capacity. Expandable size describes the ultimate capacity of the switch in terms of lines when all possible expansions have been accomplished. The expandable size is used in the calculations for air-conditioning, batteries, generator, and power.

d. Single-Line Concept - The single-line concept encompasses the requirement that each user will have a unique telephone number and a dedicated path to the telephone switch. Planners should implement single-line concept with all new construction projects, modernization projects, and routine upgrades to the voice system.

4.4.1 Factors in Choosing Distributed Switching.

a. There are several basic architectural considerations in the design, upgrade, or expansion of an Army telephone system. The designer should consider the geographical layout of the base, the availability of floor space, the existing cable routes, the existing system design, the location of the commercial telephone company point of presence, future growth, and the many other factors.

b. When at all possible, after consideration of the requirements and site survey of the location, a system design using one centrally located switching system is recommended. One centrally located switching system will serve a large number of subscribers more economically than multiple switches or remote switching units. The operation and maintenance (O&M) costs for HVAC and building maintenance will be minimized with this configuration. Software and hardware costs can be minimized if one central switch serves the maximum number of customers. The location of the central switch should be considered when siting construction for new buildings.

c. In many cases, evaluation of the site data will result in the determination that one centrally located switch can not serve the entire post. If this is the case, then a main switch with remote switching units homed to the main switch is the recommended configuration.

4.4.2 Space Limitations.

Another condition that may prohibit the installation of one central switch would be lack of floor space with no possibility of additional space at the established central office site. While it is possible to change the point of presence, the local telephone company will usually charge a hefty fee for this relocation. Long established cable routes will have to be disrupted.

4.4.3 Community of Interest.

Possible reasons or considerations for establishing a community of interest are:

a. Geographic Zones. If an area is geographically separated from the cantonment area, a remote switching unit may be more economical and easier to maintain than service from the DCO.

b. Hospital. Hospitals are treated as islands of service due to the differing types of requirements presented. Automated appointment, voice mail, and various other systems should be considered when installing a remote unit in a hospital.

c. Security Factors. Various security factors may result in the need for a remote switching unit in a building or particular area. e.g., a Special Forces compound.

d. Due to the limited range of the feature telephone, a large number of users in a single building will often require a remote switching unit in that building in order to service feature telephones, even if the building is within cable range for 2500 sets.

4.4.3.1 Multi-Vendor or Multiple Switches.

a. The O&M burden is a consideration when multiple switches are installed on a site. Each switch is considered as a separate entity by the vendor and each will require a separate software upgrade. Each type of switch (especially from different vendors) will require a separate complement of spares.

b. If optional features are to be extended across the site, the software should be purchased for all switches. Although switch networking software is being improved, there is generally some flexibility penalty to pay (i.e., reduced feature transparency across multiple switches).

c. Multiple switches also impose an administrative burden. In any given year, a number of personnel will be moved to different locations on post. If the move takes the user from the serving area of one switch into the serving area of another switch, changes will have to be made in the database of both switches, in addition to the jumper changes at two different locations.

d. Installation of switches from multiple vendors introduces various burdens in maintenance and equipment. Some of these areas include different spare complements, use of proprietary telephone sets, different software loads, different features, and different interfaces to telephone management system.

4.4.4 Type of Switch Based on Size.

There are typically two types of switching equipment that can be used for most applications.

a. For installations up to about 5,000 lines, there are several commercially available private branch exchange (PBX) switches that meet Army performance requirements. This PBX will be referred to as a Small Dial Central Office (SDCO).

b. For installations with initial sizes over 5,000 lines or for OCONUS locations, the selection of currently available PBXs with developed DISN software is much smaller. The larger switch will simply be referred to as the DCO.

The two sizes have many features in common. Both have redundant common control and supply similar user features. They differ in areas such as administrative capabilities, built-in test equipment, and trunk interfaces.

4.4.4.1 Small Dial Central Office.

a. For installations of less than 5,000 lines, small PBX equipment, with the capabilities of a PBX, as defined in Joint Interoperability and Engineering Organization (JIEO) Technical Report 8249 (Generic Switching Center Requirements), is generally installed.

b. The SDCO generally consists of one common control cabinet and a number of peripheral card cabinets. Lines and trunks are mixed within the shelves in the peripheral cabinets to load balance the system. The design is usually very compact, power efficient, and state of the art with feature laden software.

c. The main differences between the SDCO switch and the larger DCO switch are administrative capabilities and built-in diagnostics.

d. Trunking to the Defense Switched Network (DSN) is through PBX access lines. One or two specific trunks are used to support, and are reserved for only, multi-level precedence and pre-emption (MLPP). DSN interswitch trunks are not supported on the SDCO switch.

e. The maximum loop resistance design is often smaller than for the larger PBX. The loop resistance is generally dependent upon the manufacturer of the switch, but it ranges between 900 and 1500 ohms.

4.4.4.2 Dial Central Office Switch.

a. Large PBX equipment, with the capabilities of an end office, as defined in JIEO Technical Report 8249 (Generic Switching Center Requirements), is generally installed.

b. For initial installations larger than 5,000 lines (but in some cases as small as 2,000 or 3,000 lines, or for OCONUS locations). The large switch typically consists of a common control cabinet, one or more switch matrix cabinets, a miscellaneous cabinet, a number of peripheral control cabinets, a trunk cabinet, and several line card cabinets.

c. The large switch has more administrative capabilities, but not necessarily more user features. It can be programmed to perform automatic OSP cable testing during off-hours.

d. It can support DSN inter-switch trunks and thus function at a higher network level in the DISN. Any member of the DSN interswitch trunk group can be used to carry MLPP traffic.

e. Although the smaller switch product lines seem to have more rapidly adopted new manufacturing technology, the newer interfaces such as Integrated Services Digital Network (ISDN), packet, and LAN are generally fielded first and more robustly on the larger switch.

4.4.4.3 Remote Switching Unit.

a. Most PBX product lines have some kind of cabinet that can be remotely located to provide line cards for a remote group of users. This cabinet is supported by the common control in the main switch and usually connected by fiber optic cable.

b. The small PBX generally has the capability to remotely locate a cabinet of line cards over a limited distance. Most remote cabinets for the SDCO do not have stand-alone switching capability.

c. The larger switches have the capability to serve significantly larger remote switching units. They feature stand-alone switching capability in the event the links to the main switch are cut. They often support several thousand users at distances in excess of 100 miles.

1. All features available to the main switch subscribers are supported. Features are transparent to all users (same control codes).

2. Trunking is supported for local city trunks for backdoor connectivity (mainly for emergency).

3. In the stand alone mode, as occurs when links are cut, the remote switching unit does not have access to the software in the main switch; therefore, service is limited to Plain Old Telephone Service (POTS). Most of the control software for MLPP and ISDN resides at the main switch.

4. There are usually dialing plan restrictions that effect portability of numbers if standalone support is desired. Because of the programming complexity, stand-alone capability is only recommended for users who absolutely need immediate local telephone service.

d. Some large switches also support simple remote shelves similar to the capabilities of the smaller switch. These shelves can generally be remoted using standard multiplexing equipment. The shelves usually have no stand-alone switching capability and may or may not support electronic features or ISDN telephone instruments.

4.4.4.4 RSU vs. SLC.

a. Subscriber loop carrier (SLC) is now supported on several larger switches through direct interface. That is, the switch has software that allows standard remote terminal (RT) equipment to interface directly with switch T1 interface cards without the need for central office terminals (COT), line cabinets, line cards, or frame jumpers.

b. Since this interface at the switch side is still copper T1, there must be some sort of compatible multiplexer between the switch and the OSP cable. But line cabinets and distribution frame space are not needed, so there is generally a space savings in the switch room and a cost savings in line equipment if the RT already exists. This interface is now standardized.

4.4.5 Connectivity Between Nodes.

There are at least three different technologies in common use at this time: copper T-carrier, fiber optic DS3, and fiber optic Synchronous Optical Network (SONET).

4.4.5.1 Copper T-Carrier.

New systems seldom use copper T-carrier, although it is possible that a small upgrade to an existing system will have to use T-carrier for logistics reasons.

4.4.5.2 Fiber Optic DS3.

Most switching systems require DS1 transmission between the main switch and the remote switching units. Transmission systems have been installed for many years that transmit one, two, or three DS3 signals over fiber optic cable between those two points. Multiplexer shelves break the high-speed signal (45, 90, or 150 megabits) into multiple DS1s for interface to the switch. At the present time, fiber optic DS3 systems are generally only used as small upgrades to existing systems.

4.4.5.3 Fiber Optic SONET Ring.

a. Most manufacturers have ring software for their SONET hardware. If ring software is in use, a break in the active fiber optic cable will not cause an outage, traffic will be automatically rerouted via an alternate cable.

b. SONET is a standards based architecture. Theoretically, SONET multiplexers from different manufacturers are interoperable. However, many manufacturers use different methods of implementing ring software. If a ring is to be implemented, all equipment should be the same model and use the same software.

c. SONET rings require fiber optic cable routes that are diversely routed and physically connect the outlying sites into the ring. On a large installation, the cost of the fiber optic cable to complete the ring can total millions of dollars.

d. The problem is further compounded on larger sites by capacity issues. The ring architecture requires the entire ring to have the bandwidth to carry the sum of all the payloads of each remote site operating on the ring. At a small site with less than four nodes, a single OC12 system can be used to provide a ring. The advantage of this design is that the equipment in the central office is minimized. Only one chassis is required at the main switch to provide for four nodes.

4.4.5.4 Fiber Optic SONET Star.

a. SONET equipment operated in a star configuration is recommended for the transmission system. This architecture can generally be implemented at reasonable cost.

b. The star wired architecture is very compatible with the structured wiring used by OSCAR-II for the copper distribution cables. It provides reasonable reliability at reasonable cost. Since each arm is required to carry only the traffic between the main switch and one node, ultra high-speed equipment is not needed.

c. The architecture also fits well with the design used by CUITN, so cable costs are minimized.

d. Using the star architecture also eliminates the problem of proprietary ring software. Equipment from different manufacturers can safely be mixed in the system, eliminating dependence on one vendor and allowing future replacement of equipment a piece at a time.

4.4.6 Telephone End Equipment.

The following paragraphs discuss instrument distance from the servicing switch and features including portability

4.4.6.1 Distance Limitations.

Standard 2500 sets and ISDN instruments can be located up to 18,000 feet from the serving switch, depending on wire gauge and loss, whereas electronic feature telephones generally have shorter reach (3,000 feet).

4.4.6.2 Features.

Electronic feature telephones and ISDN telephones are attractive to many users because they provide programmable feature buttons for ease of use and multiple lines. The additional lines, of course, are electronic and only provisioned in software. The instrument is served by only one or two pairs of wire regardless of the number of line appearances. The electronic feature telephone interface is generally proprietary in nature while the ISDN set is standard, but the feature telephone is often one half to one third of the cost of an ISDN set and is therefore more often chosen.

4.4.6.3 Portability.

The feature telephone can only be used on the model switch for which it was designed and so it can not be moved from post to post unless both posts have the same switch type. There can be problems moving even ISDN telephone sets from post to post. The early models were not interchangeable because the programming of the multiple buttons was not standardized.

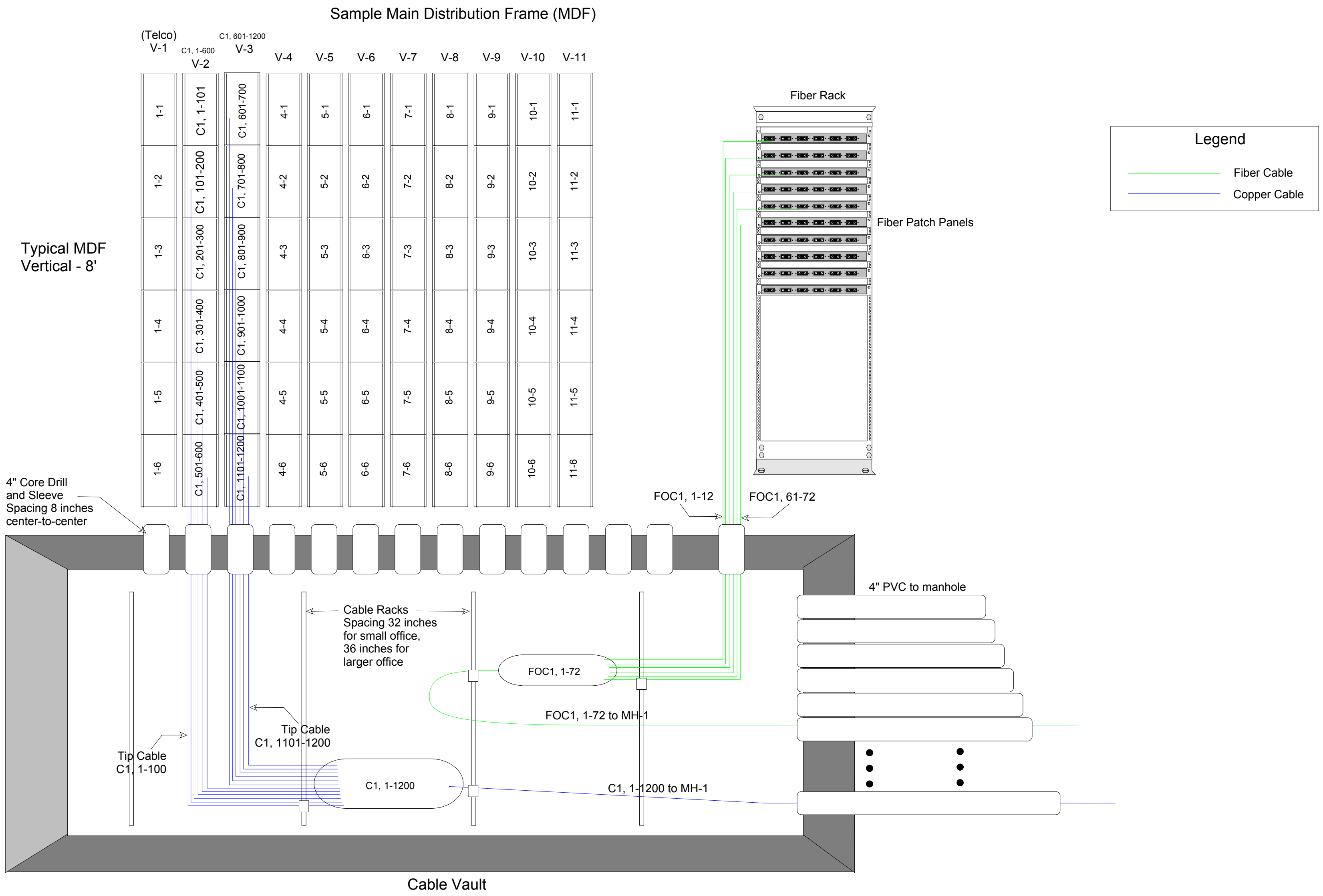


Figure 4-1: MDF and Cable Vault Schematic

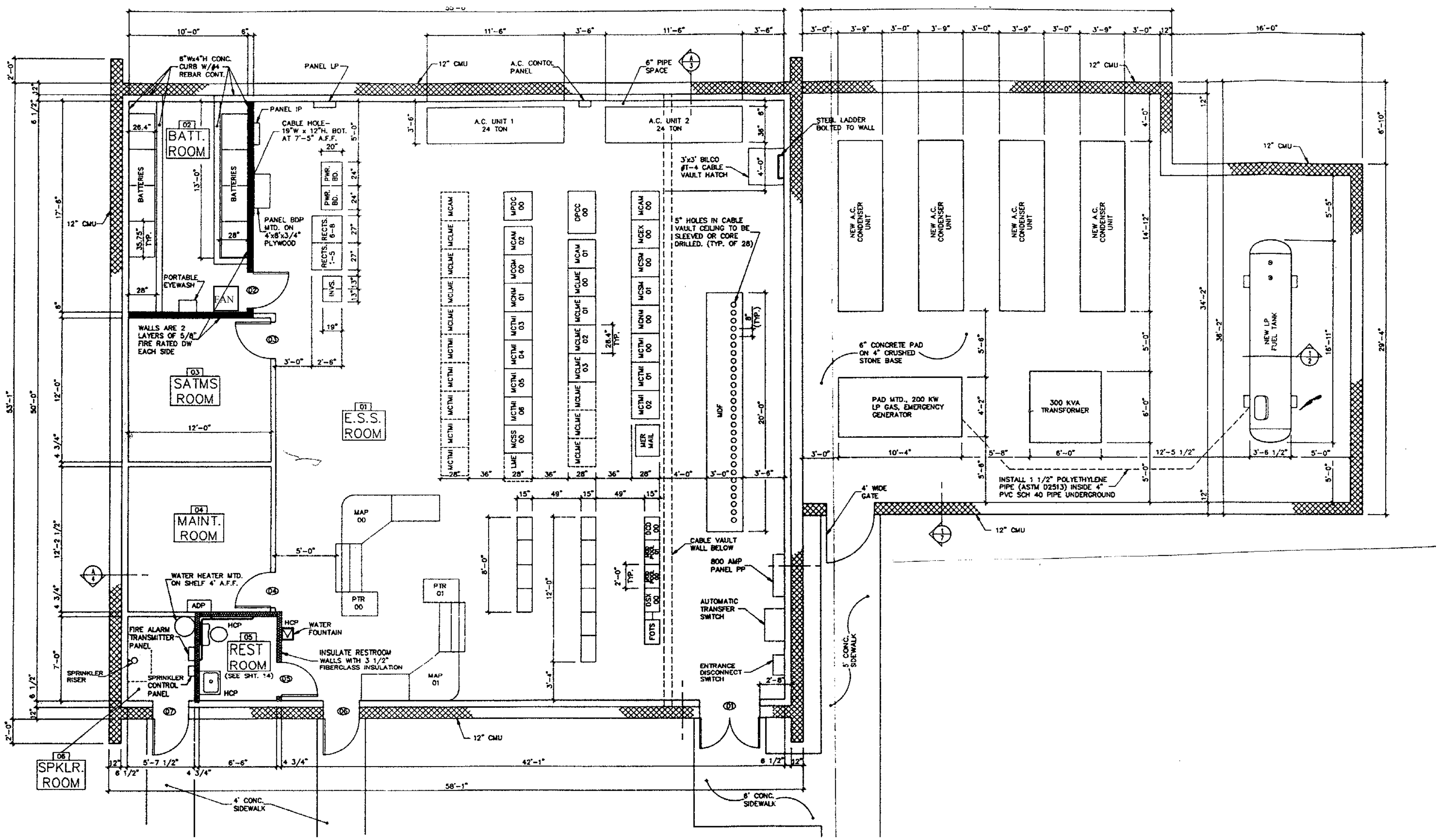


Figure 4-2: Typical Switch Room Layout

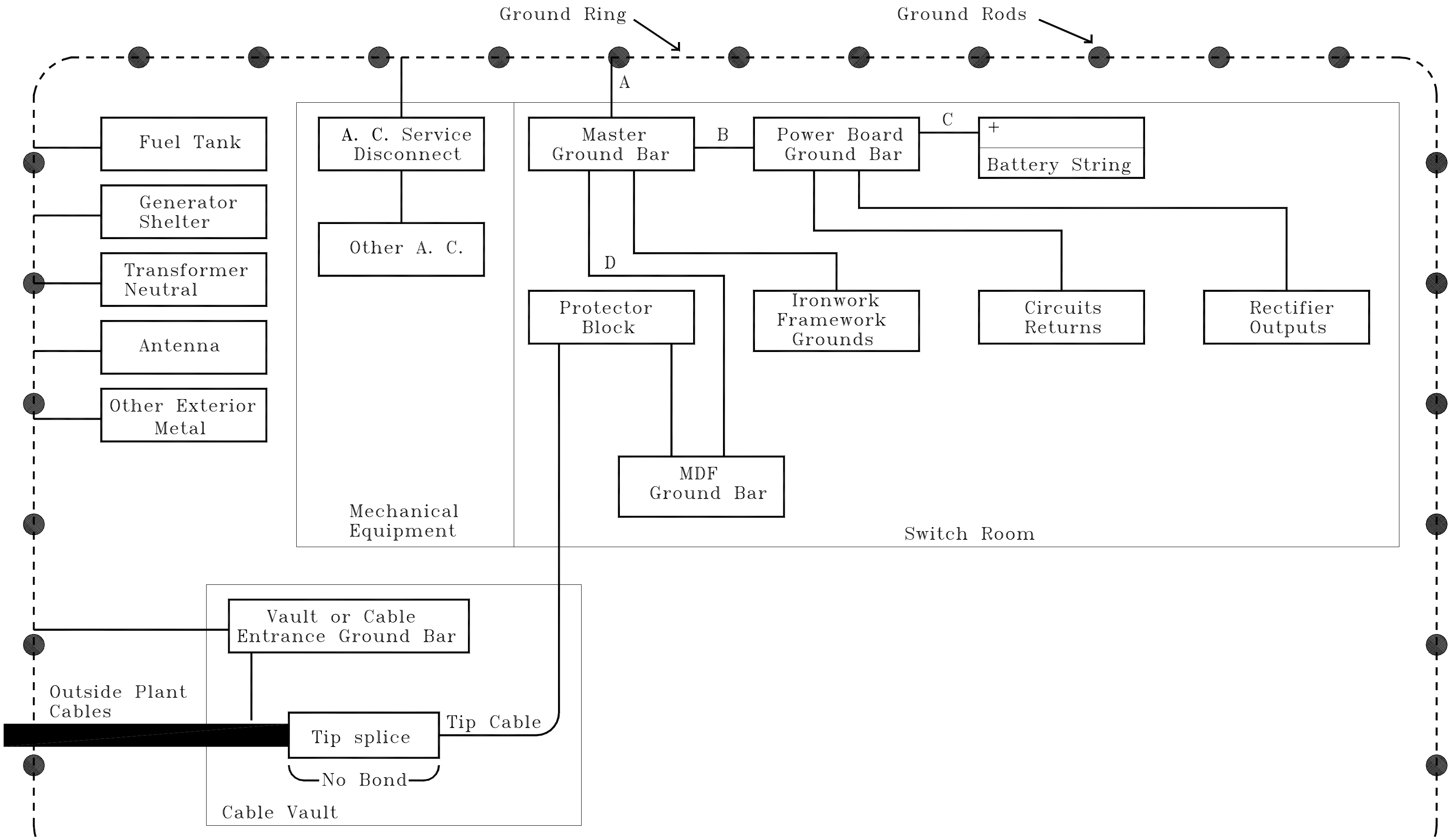


Figure 4-3: Grounding Schematic

5.0 NETWORK ARCHITECTURE

5.1 Network.

The planned network architecture is based on data switches at the MCN, ADN and edge devices at the EUBs. The transport technology has been ATM, however, GbE is now an approved alternative. These edge devices allow attachment of legacy switched or shared media LANs, by emulating the legacy protocols over the networks. Routers can be used to interface to non-Ethernet legacy LANs, like FDDI or token-ring, and to interconnect the emulated LANs created on top of the network.

5.2 Nodes.

The nodes of the installation telecommunications network consist of the MCNs, ADN, and primary and secondary EUB entrance facilities. Details on the TR and user work locations/work areas are found in the Premise Distribution Systems section.

5.2.1 Main Communication Node.

The MCN houses the main telephone switch, installation MDF, wide area network (WAN) gateway, primary installation backbone network switch, and ADN-level switch for connecting to primary EUB TRs in its local service area. Figure 5-1: Main Communications Node depicts a typical MCN. The alternate MCN houses a secondary telephone switch or RSU, alternate WAN gateway, the alternate installation backbone network switch, and ADN-level switch for connections to primary EUB TRs in its local service area. Collocating the data network equipment with the central telephone switch allows for the use of the existing manholes, duct system, and fiber cable plant, and provides the ability to integrate the telephone and data backbone networks when the technology becomes available. The MCN installation backbone switch interconnects the A-MCN and all ADN backbone switches.

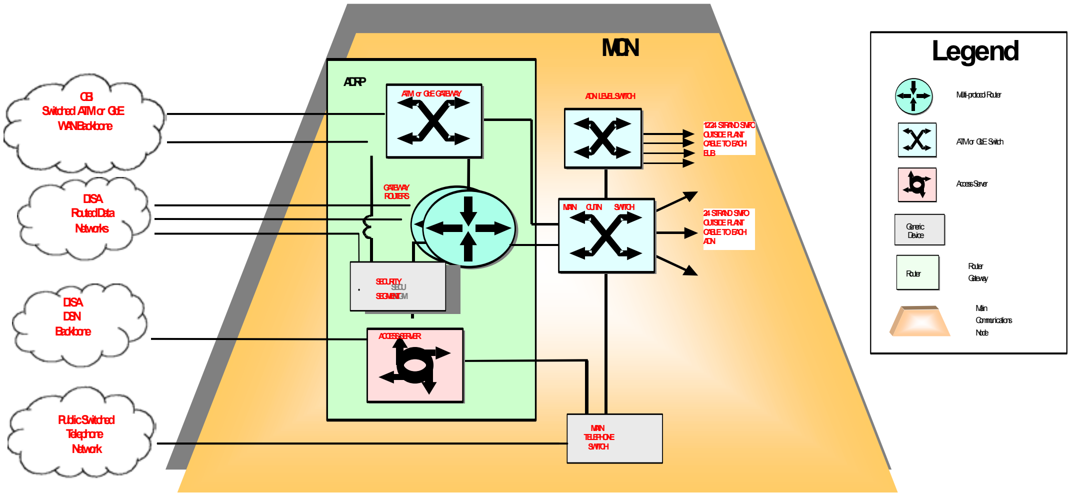


Figure 5-1: Main Communications Node

5.2.1.1 MCN Switches.

For GbE networks, the main switch will be located at the MCN with 1000 megabits per second (Mb/s) single-mode fiber optic connection to the ADNs. For an ATM network, the ATM switch is typically located at the MCN and provides interconnectivity to the ADNs via point-to-point ATM link at a minimum rate of OC-3c (155 Mb/s).

5.2.1.2 Alternate MCN.

The A-MCN at each site should provide full backup to the MCN, with a full suite of standby equipment with automatic switch-over. The A-MCN should be configured and connected to the ADNs identically to the MCN.

5.2.1.3 Maximizing Existing Resources.

Any installation data communication network that is deployed (e.g., CUITN) should be collocated with the existing telecommunications resources. This allows for utilization of existing manhole and duct systems, cable plant, human resources, and most significantly, the ability to utilize network resources when the telecommunication and data communication networks become integrated onto one backbone network. Figure 5-1: Main Communications Node depicts an MCN interconnection.

5.2.2 Area Distribution Node.

a. ADNs house the data network switches and, if required, the telephone RSU. They are connected to the main switches in the MCN and to switches/edge devices/hubs in each TR serviced by the ADN (Figure 5-2: Area Distribution Node). The telephone RSU and data switches/hubs should be collocated in ADNs to concentrate the cabling and traffic from user systems in the EUBs. Locations for ADNs should be based on both geographical considerations as well as the traffic load from the users. The maximum distance between the ADN and any customer station may not exceed a specified distance based on technology consideration cost trade-off. (Note: The current policy is for a nominal 10,000 to 13,500 feet and not to exceed 18,000 feet. These distances are based on signaling limitations of the data and telephone technologies as well as cable consolidation considerations.)

b. ADNs provide backbone connectivity via data switches to the EUBs over fiber optic links. The equipment located at the ADNs should be able to provide connectivity for legacy systems as well as a migration path to future technologies. The data switch at the ADN connects the switches/edge devices/hub located in the EUB TR to the network backbone via OC-3c or higher links. ADNs will also house one-armed routers and LANE services devices, when required for support of legacy LANs.

c. The switches at all ADNs should be connected to both the primary MCN and the A-MCN. This interconnection configuration provides robust connection for capacity, scalability, full throughput, and redundancy. Every ADN should have a direct connection to the MCNs and at least two other ADNs. Reference paragraph 3.4.2and subparagraphs of the OSP for fiber cable sizing.

5.2.3 End User Building Entrance Facility.

The following paragraphs address both Primary and Secondary EUBs.

5.2.3.1 Primary EUB TR.

Primary EUB TRs support a full complement of data users (nominally 50), and are the termination point for the horizontal wiring with a maximum distance of 295 feet from the TR to the wall outlet. EUB TRs may concentrate telecommunications network connections from surrounding secondary EUB TRs in order to provide a cost effective distribution network.

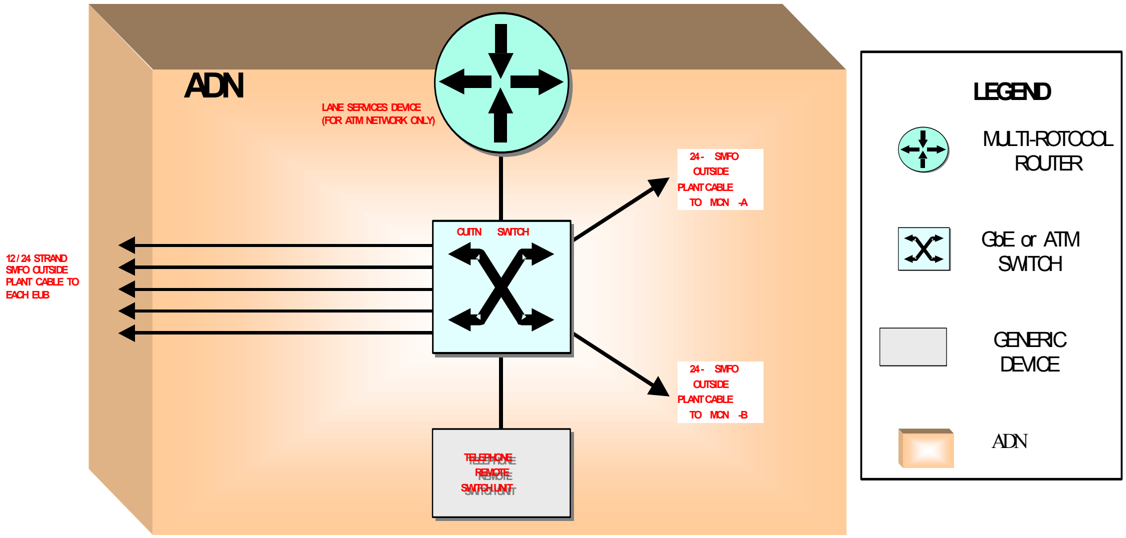

ADN
LANE SERVICES DEVICE
(FOR ATM NETWORK ONLY)
24- SMFO OUTSIDE PLANT CABLE TO MCN -A
CUITN SWITCH
12/24 STRAND SMFO OUTSIDE PLANT CABLE TO EACH EUB
24- SMFO OUTSIDE PLANT CABLE TO MCN -B
TELEPHONE REMOTE SWITCH UNIT
LEGEND
MULTI-ROTOCOL ROUTER
GbE or ATM SWITCH
GENERIC DEVICE
ADN

Figure 5-2: Area Distribution Node

5.2.3.2 Secondary EUB TR.

Secondary EUB TRs support a separate complement of data users. The maximum distance limitation of 295 feet from TR to wall outlet still applies. Secondary EUB TRs are connected to the edge device in the primary EUB TR for connection to the installation network. This configuration supports efficient cable and equipment utilization.

5.2.3.3 Customer Premises LAN.

The preferred customer premises LAN is a data hub connected to an GbE edge device located in the TR with horizontal wiring to the user workstations and single-mode fiber riser cable to the other TRs and single-mode fiber OSP cable to the ADN. The EUB data hubs should be of modular design to allow for growth in size and changes in technologies and bandwidth.

5.2.3.4 Typical EUB LAN Components and Characteristics.

a. Figure 5-8: Typical LAN, shows the recommended basic components for an EUB. Stackable or small modular chassis can be used as noted on the sketch, for small user population with a small potential for growth. Uplink or high speed interfaces on the stackable hubs should be modular to allow for changes in connection speeds.

b. EUB LANs can consist of existing 10BaseT shared Ethernet. Switched 10 and 100 Mb Ethernet are now widely available, with Gigabit Ethernet also emerging for building and small campus environments. The US Army is currently migrating away from Token Ring, and the designer should consider replacing the Token Ring LAN with an 802.x switched network. Some general guidelines for designing and implementing EUB LANs are:

1. The equipment and hardware will be from manufacturers that have a minimum of 3 years experience in producing the types of systems and equipment specified.

2. The equipment should adhere to current or emerging standards accepted by the industry (802.x, etc.).

3. The LAN electronics and software should be fully compatible and interoperable with the existing EUB equipment, if the EUB equipment is not to be replaced.

4. Obsolete items or items no longer supported by the manufacturer should not be utilized to fulfill the requirements in the EUB.

5.3 Description of Networks.

Campus area networks (CANs) utilize a backbone (normally fiber optic cable,) to interconnect the LANs in several buildings or groups of buildings within a local area, such as an Army post. Metropolitan area networks (MANs), interconnect several CANs and/or LANs usually with leased commercial lines (normally fiber optic cable) over a larger area or region such as the Army installations in the Military District of Washington. WANs interconnect LANs, CANs, and MANs through a non-homogeneous mix of transport media and communications protocols, encompassing national or international areas. WANs offer a wide range of services (such as DISN and commercial services) normally not available in smaller networks. Additional information can be found on the CUITN web-site (https://cuitn.hqisec.army.mil/).

5.4 Topology.

Network topology may be Mesh or Partial Mesh configuration.

5.4.1 Mesh Connections.

The installation backbone network should be connected in a partial mesh topology for optimum configuration with switched technologies (for GbE and ATM). Interim logical bus or ring topologies can be configured using the physical star topology. The mesh connections provide survivability and load leveling.

5.4.2 Partial Mesh.

A partial mesh should be used to maintain scaleable-switched environment. At a minimum, all ADNs should have connections to both the primary and alternate MCNs and two adjacent ADNs. Figure 5-3a shows the partial ATM mesh topology whereas Figure 5-3b shows the preferred partial GigaBit Ethernet mesh topology.

5.4.3 Dual Connectivity.

The required full time availability is achieved by using primary and alternate MCNs and connecting each ADN to both MCNs. This supports the capacity required out of each ADN and provides the required full time availability. It is highly desirable to provide diverse fiber optic cable routings so that a single cable cut/break will not prohibit ADN connections to an MCN.

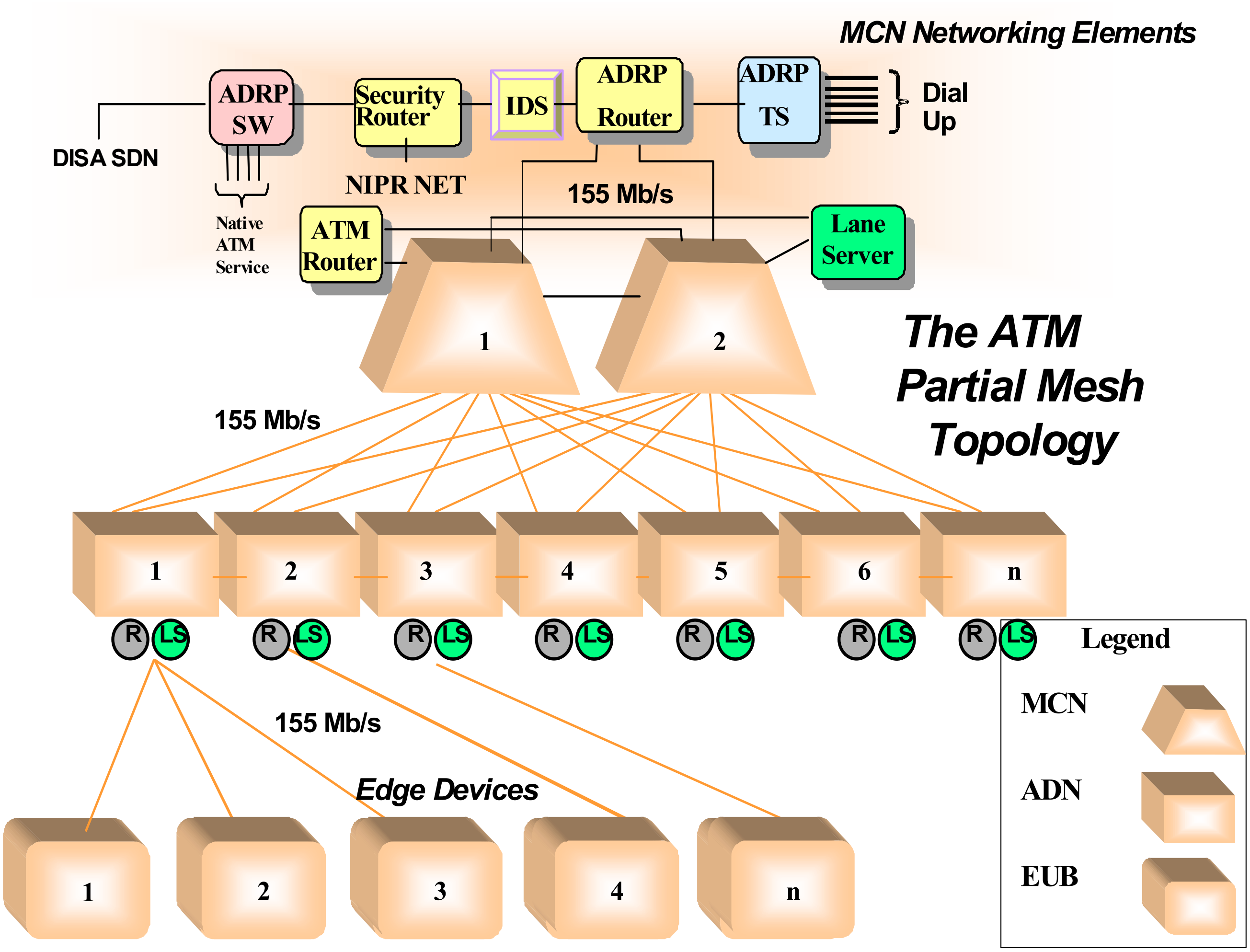


Figure 5-3a: Partial ATM Mesh Topology

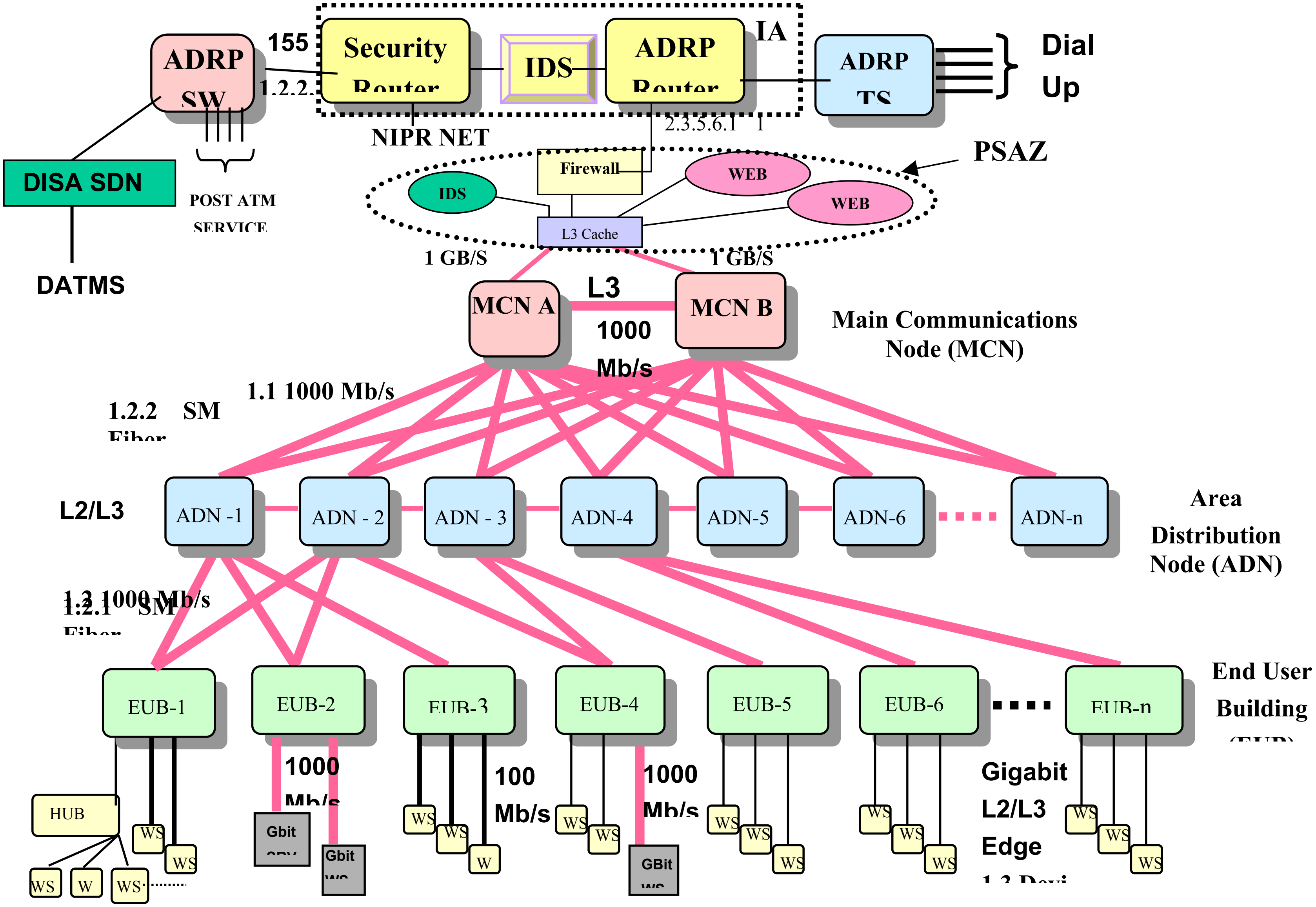


Figure 5-3b: Switched GbE Partial Mesh Topology

5.5 Local Area Network.

On a post the LANs are data networks that normally serve an EUB and in some instances serve a limited number of EUBs. Normal LANs are designed to only serve an area that is a few square kilometers.

5.5.1 LAN Configuration.

Within an EUB there are many options available in configuring a LAN. Depending on the number of end users, LANs may stretch across buildings. In most cases, a LAN will be established in each EUB and support about 25 to 150 end users. When EUBs have fewer than 25 users they can be tied into other EUBs and their LAN. Keeping the size of the LAN to a limited number allows optimizations to be made favoring greater data rates and placing less pressure on centrally located servers. An example of the recommended LAN topology is shown in

Figure 5-4: LAN Topology. In this topology an EUB stacks hubs in a telecommunications room supporting one to the variable number of floors in the building. Using this topology centralizes communications troubleshooting while isolating different floors of the LAN.

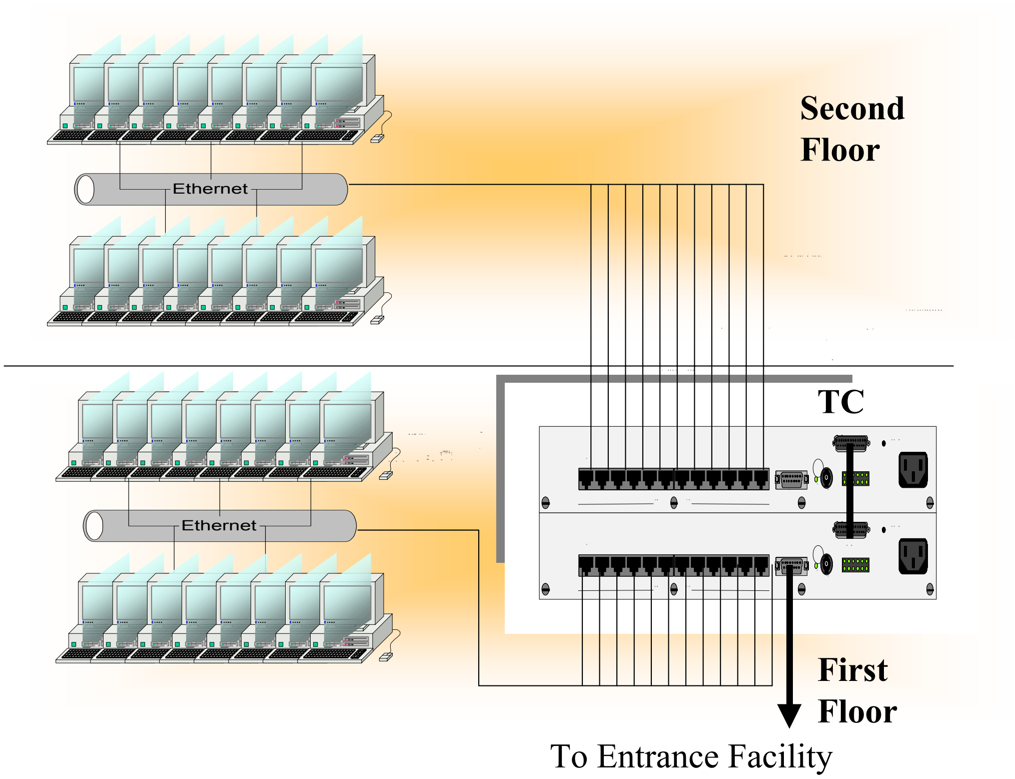


Figure 5-4: LAN Topology

5.6 Alternate Types of LANs.

The following paragraphs describe alternate types of LANs.

5.6.1 Multimode Fiber Optics LAN.

The internal LAN cable plant will consist of UTP Cat 5 cable or multi-mode fiber optic cable from the hub to the end user device. When using fiber optic cabling, the Building Entrance Facility will connect directly to the hub. Placing fiber optic patch panels within the TR may increase decibel (dB) loss affecting the performance of the fiber. Limit the number of splices necessary in any LAN, but especially using fiber optic cabling. Multimode fiber optics to the end user devices can be used in the LAN with either an edge device or a hub. To connect to an Ethernet hub you must have a fiber card in the hub or use an Ethernet to fiber optic transceiver. Figure 5-5. LAN Using Multimode Fiber Optics is a diagram of a LAN using multimode fiber optic cabling and an edge device. Only single-mode fiber will be used for riser cable.

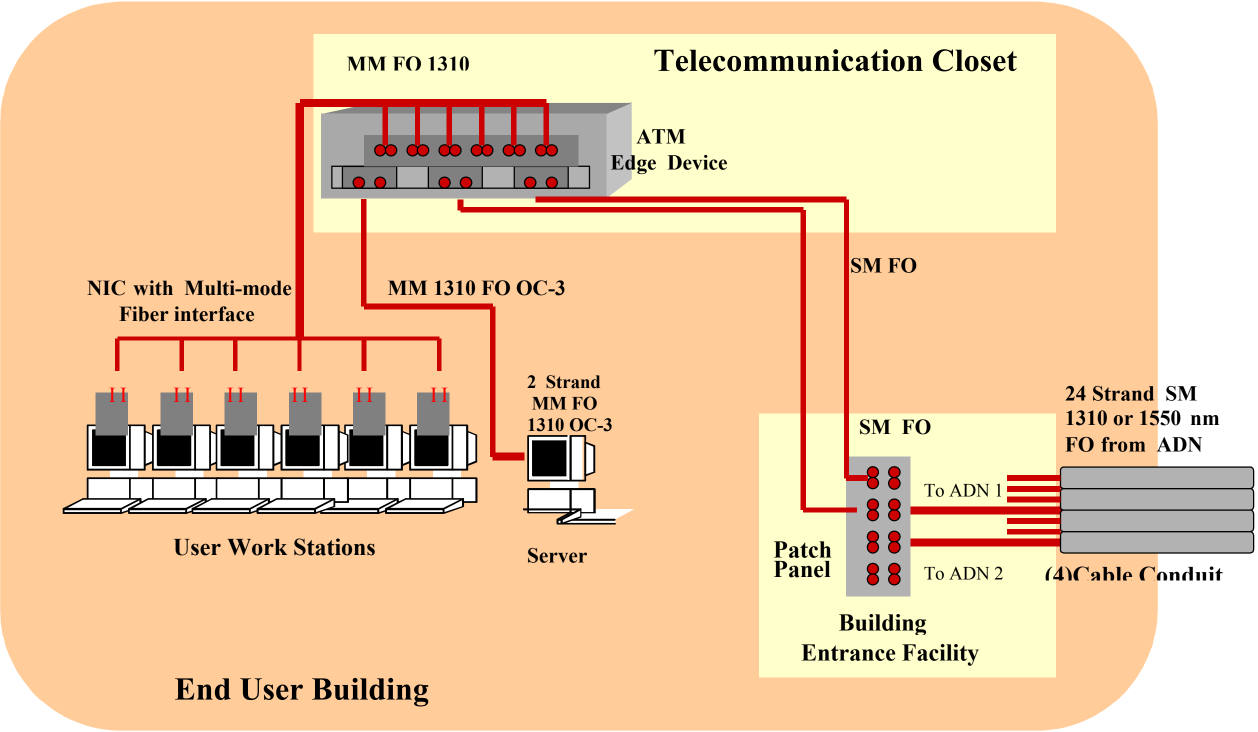


Figure 5-5. LAN Using Multimode Fiber Optics

5.6.2 Fiber Distributed Data Interface LAN.

In cases where there is limited funding available to procure current data networking hardware designers can make use of existing routers. Routers that were initially placed on the backbone of a network and removed when the network was upgraded, can be moved down to an EUB and used with Fiber Distributed Data Interface (FDDI) to improve the performance of a LAN. In order to do this it is necessary to have or install single-mode fiber optic cabling from the EUB entrance facility into the router and between multiple routers used within the LAN. Figure 5-6: LAN Using FDDI shows a typical FDDI LAN.

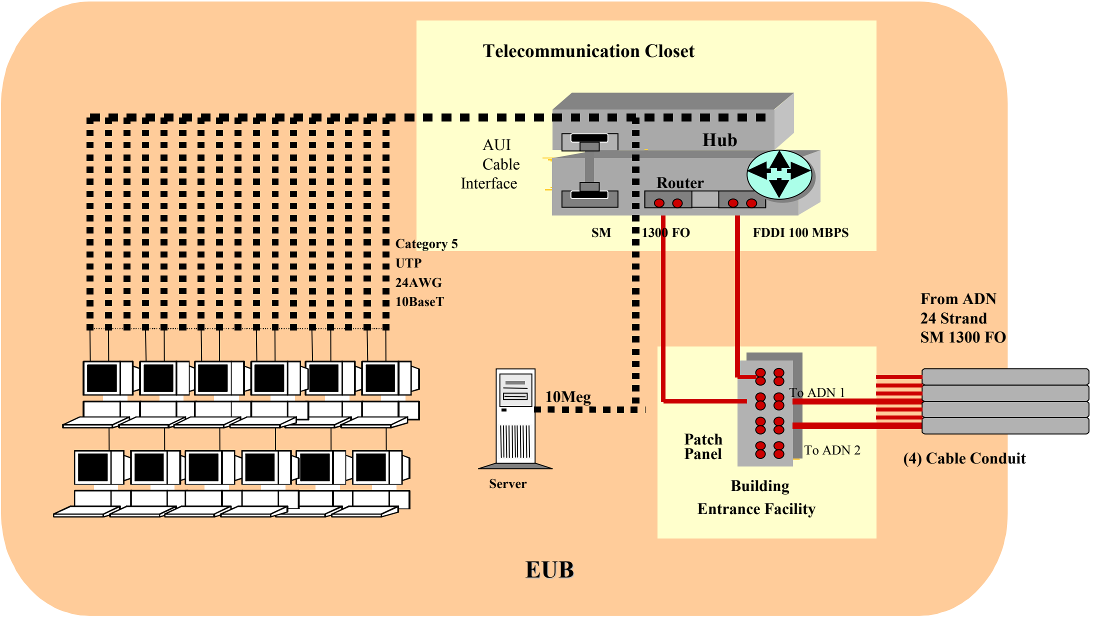


Figure 5-6: LAN Using FDDI

5.6.3 T1 Wire Line LAN.

One way to connect buildings that do not meet the minimum essential requirement qualifications, but still need network connectivity is using a T1. A T1 connection can be made via the voice backbone using a Digital Service Unit/Channel Service Unit (DSU/CSU) into a router. This defers cost from additional cable plant installations for data connectivity. The DSU/CSU connects to the voice patch panel via UTP and requires two pair. From the DSU/CSU a connection is made using a serial cable into a serial port on a router. The router then connects into a hub that provides Ethernet service to end users. A depiction or a T1 Wire line LAN is shown in Figure 5-7: LAN Using T1 Wire Line.

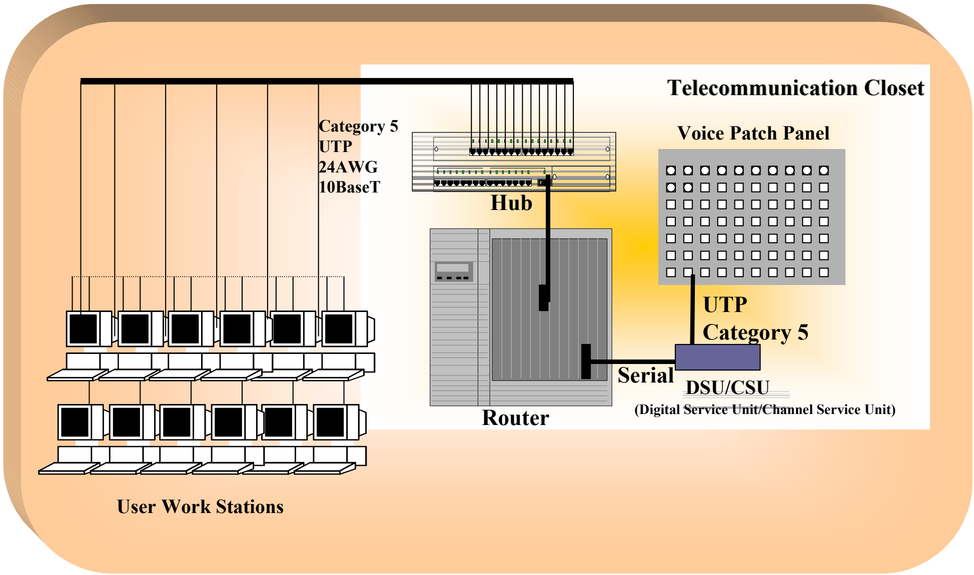


Figure 5-7: LAN Using T1 Wire Line

5.7 Growth.

All equipment hubs (including routers and switches) will be designed with at least a 25 percent growth factor to support future system enhancements. In addition, fiber optic cable installations will be of sufficient quantity to accommodate at least a 100 percent increase in requirements.

5.8 Interfaces.

The following paragraphs pertain to both new installation and legacy system data interfaces.

5.8.1 Data Interface.

a. The primary data interface between the ADN and the TR is an ATM/SONET OC-3 or GbE signal on single-mode fiber optic cable operating at 1310 or 1550 nanometers (nm). Two separate fiber connections are required, one for transmit and one for receive.

b. The primary host/server interface at the ADN is an Institute of Electrical and Electronics Engineers (IEEE) 802.3 10BaseFL on multimode fiber optic cable (horizontal wiring operating at 850 and 1310 nm).

c. The projected future host/server interface at the ADN is a 100-Mb/s IEEE 802.X or an ATM/SONET OC-3c signal on multimode fiber optic cable (horizontal wiring operating at 850 and 1310 nm) or Cat 6 UTP.

d. The preferred connector for fiber optic cable is an SC connector. An alternative data interface for existing multimode fiber optic cable is an IEEE 802.3 signal at an ST connector on multimode fiber optic cable operating at 850 and 1310 nm.

5.8.2 Legacy System Data Interfaces.

a. An alternative legacy LAN/host/server data interface is a FDDI at a network interface card (NIC) dual fiber connector on multimode fiber optic cable operating at 850 and 1310 nm. The multimode fiber optic cable is used for horizontal cabling to host computers or gateway devices at the ADN. Optionally, this provides the interface to FDDI subnetworks using existing multimode fiber optic cable.

b. An optional legacy LAN data interface is to extend the FDDI to a distant TR using single-mode fiber optic cable operating at 1310 and 1550 nm. Four separate connections using ST connectors are required for transmit and receive on both the "A" and "B" FDDI rings. Compatible single-mode equipment is required at both the TR and the ADN.

c. An alternative interface for legacy equipment with T1/T3 interfaces is an ATM cell adaptation multiplexer which converts the T1/T3 signal to an ATM/SONET OC-3c signal at an ST connector on single-mode fiber optic cable operating at 1310 and 1550 nm.

5.8.3 User Interface

Users will interface with the network system from workstations. Connection to the individual workstation will be through the EUB LAN as described above, and the PDS. The EUB LAN is connected to the network backbone through the edge device.

5.9 Connection to OSP

Data switches and edge devices connect to the OSP through the single-mode fiber optic patch panel installed as part of the OSP distribution system. The single-mode patch panel description and locations are specified in the PDS and OSP sections of this document. The data switches and edge devices should be collocated with the single-mode fiber optic patch panels in order to avoid having to run an extension of the fiber cabling.

5.10 Digital Subscriber Line Technology.

Digital Subscriber Line (xDSL) describes a family of new modem technologies that convert existing twisted-pair telephone lines into access paths for multimedia and high-speed data communications. The significant advantage that xDSL offers to users is an economical means of substantially increasing bandwidth in small offices. Therefore, xDSL may be an option for sites that are not connected to an installation infrastructure, and with limited connections, such as Reserve and Guard Units. xDSL implementations can support downstream rates ranging from 1-52Mb/s and downstream rates ranging from 512Kb/s to 34Mb/s Such rates expand existing access capacity without new cabling. xDSL can literally transform the information network from one limited to voice, text, and low resolution graphics to a powerful system capable of bringing multimedia, including full motion video, to every building.

5.11 Wireless Connections and Technology.

Current wireless LANs use one of three technologies, narrowband radio frequency (RF) signaling, spread spectrum RF signaling, and infrared light signaling as the medium between computers, the web, or each other. The wireless LAN can be connected to an existing wired LAN as an extension, or can form the basis of a new network. Data rates for the most widespread commercial wireless LANs are in the 1.6 Mb/s range, with some reaching rates as high as 11 Mb/s.

5.11.1 Elements of Wireless LAN.

Three elements make up a wireless LAN: the distribution system, the access point and the portable unit or station. The distribution system will typically be an Ethernet or Token Ring wired LAN, which forms the backbone of the system. The access point is a stationary transceiver attached to a wired LAN that serves as a wired to wireless LAN bridge, or to the backbone of a wired Ethernet LAN via a simple cable. The portable unit or station can be a personal computer (PC), notebook, or any other type of input/output (I/O) device.

5.11.2 Cell.

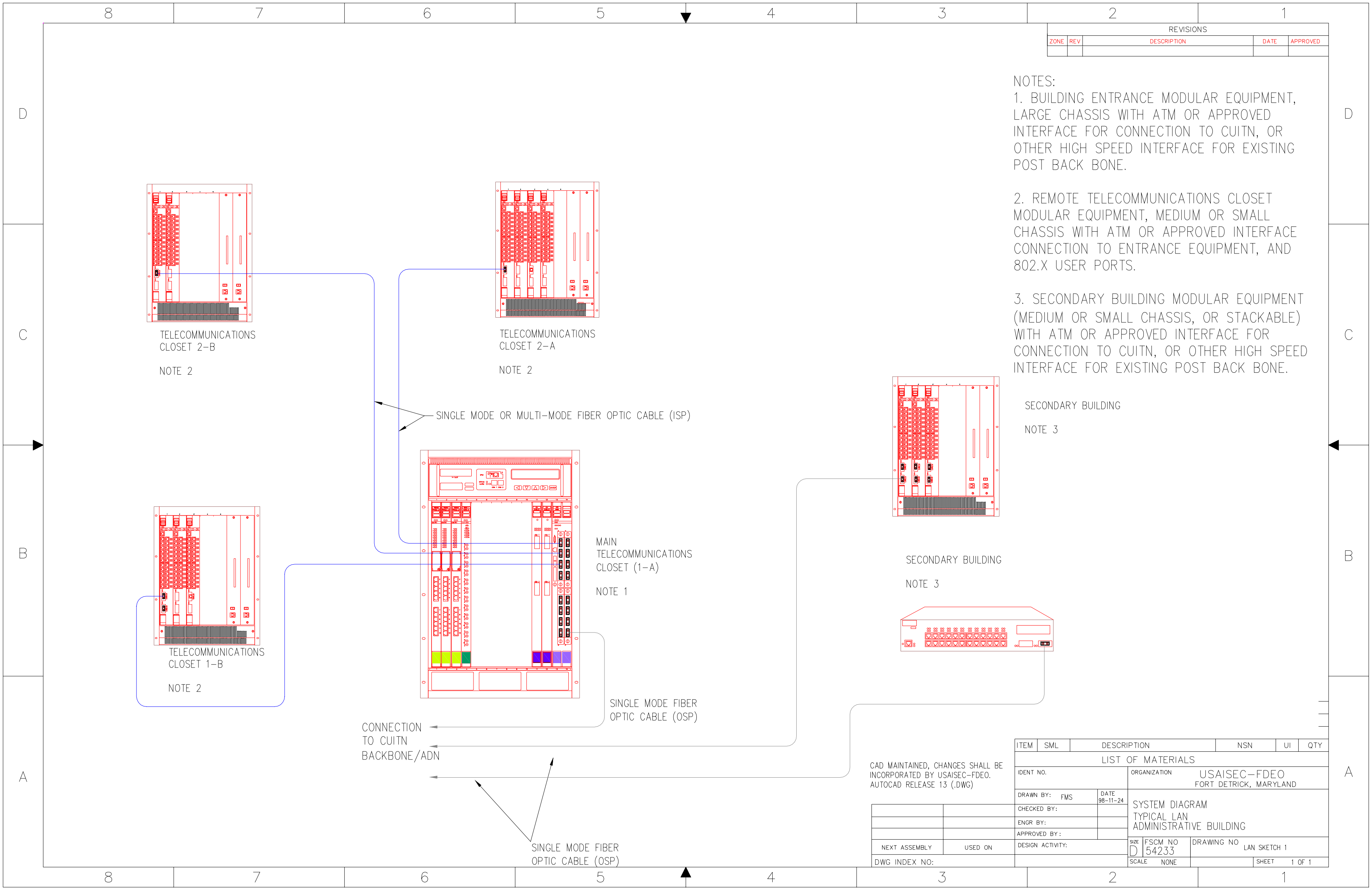
The basic building block of the wireless LAN is the "cell". This is the area in which the wireless communication takes place. The coverage area of a cell depends upon the strength of the propagated radio signal and the type and construction of walls, partitions, and other physical characteristics of the environment.

5.11.3 Access Point.

The access point connects the cells of the wireless LAN with one another and connects wireless LAN cells to a wired Ethernet LAN via a cable connection to an Ethernet LAN outlet. The basic cell comprises an access point and all the associated wireless stations. The number of wireless stations per cell depends on the amount and type of data traffic. In a "busy" environment a cell might contain 50 stations while in a more "relaxed" environment 200 stations might be supported. A stand-alone cell is an ideal method of setting up a small to medium sized wireless LAN between a number of workstations or workgroups. This type of cell requires no cabling. The stations communicate with each other via the access point, which manages the data traffic in the cell. The access point functions as a bridge between the cell and the wired LAN. Stations in the cell and in other linked cells can now access all the wired LAN facilities.

5.11.4 Standards.

Standards for wireless networking are included in IEEE 802.11.


8
7
6
5
4
3
2
1
D
C
B
A
REVISIONS
ZONE
REV
DESCRIPTION
DATE
APPROVED
TELECOMMUNICATIONS CLOSET 2–B
NOTE 2
TELECOMMUNICATIONS CLOSET 2–A
NOTE 2
SINGLE MODE OR MULTI–MODE FIBER OPTIC CABLE (ISP)
MAIN TELECOMMUNICATIONS CLOSET (1–A)
NOTE 1
TELECOMMUNICATIONS CLOSET 1–B
NOTE 2
SECONDARY BUILDING
NOTE 3
SECONDARY BUILDING
NOTE 3
SINGLE MODE FIBER OPTIC CABLE (OSP)
CONNECTION TO CUITN BACKBONE/ADN
SINGLE MODE FIBER OPTIC CABLE (OSP)

NOTES:

1. BUILDING ENTRANCE MODULAR EQUIPMENT, LARGE CHASSIS WITH ATM OR APPROVED INTERFACE FOR CONNECTION TO CUITN, OR OTHER HIGH SPEED INTERFACE FOR EXISTING POST BACK BONE.

2. REMOTE TELECOMMUNICATIONS CLOSET MODULAR EQUIPMENT, MEDIUM OR SMALL CHASSIS WITH ATM OR APPROVED INTERFACE CONNECTION TO ENTRANCE EQUIPMENT, AND 802.X USER PORTS.

3. SECONDARY BUILDING MODULAR EQUIPMENT (MEDIUM OR SMALL CHASSIS, OR STACKABLE) WITH ATM OR APPROVED INTERFACE FOR CONNECTION TO CUITN, OR OTHER HIGH SPEED INTERFACE FOR EXISTING POST BACK BONE.

CAD MAINTAINED, CHANGES SHALL BE
INCORPORATED BY USAISEC–FDEO.
AUTOCAD RELEASE 13 (.DWG)

ITEM	SML	DESCRIPTION	NSN	UI	QTY

LIST OF MATERIALS

IDENT NO.

ORGANIZATION USAISEC–FDEO
FORT DETRICK, MARYLAND

DRAWN BY: FMS
DATE 98-11-24

CHECKED BY:

ENGR BY:

APPROVED BY:

DESIGN ACTIVITY:

SYSTEM DIAGRAM
TYPICAL LAN
ADMINISTRATIVE BUILDING

NEXT ASSEMBLY
USED ON

DWG INDEX NO:

SIZE D
FSCM NO 54233
DRAWING NO LAN SKETCH 1

SCALE NONE
SHEET 1 OF 1

Figure 5-8: Typical LAN, Administrative

6.0 NETWORK AND SYSTEMS MANAGEMENT

6.1 Introduction

System and network management is becoming increasingly important in today's environment of distributed applications and heightened security. Network and system administrators rely heavily on automated Network and Systems Management (NSM) tools for tasks such as discovering, diagnosing and correcting problems, updating software, and maintaining network/system operations. Managing networks and systems is a difficult and complicated task requiring extensive knowledge in numerous areas such as operating systems, networking devices and protocols, addressing, databases, applications, and others. NSM systems are intended to ease the burden on resources associated with these tasks.

6.1.1 NSM Objectives

The objective of an NSM is to provide effective, responsive, and proactive management of networks and systems with minimal life-cycle support costs. This includes the integration of lower level management systems and subsystems to provide an enterprise view of the network and system assets. The primary uses of NSM are:

- Provide backup and recovery services
- Monitor, identify, track, and correct information system and network communication failures
- Monitor, identify, and correct network and system security problems
- Monitor, control, and fine tune network and systems performance
- Identify communication and processing resource usage
- Manage inventory and distribute software

6.2 Army Guidance and Requirements

The following guidelines apply to the development of new Army information systems.

- An NSM approach will be defined for each information system developed.
- Hardware and software will be in accordance with (IAW) the Joint Technical Architecture – Army (JTA-A) requirements to standardize management of components across the U.S. Army enterprise. In addition, installation servers will have commercial off the shelf (COTS) system management agents to allow remote management of system components in the functional areas of fault, configuration, accounting, performance, and security as required.
- Legacy systems will migrate to JTA-A standards unless a cost analysis indicates that doing so would not be cost effective and/or would not provide significant operational advantages.
- COTS software and hardware will be used to the greatest extent possible.
- Critical management functions to be performed and system interface requirements should be identified before making a product selection. This includes development of associated NSM business rules that define the operation of the management system.
- To minimize life-cycle maintenance costs, NSM applications should be customized only when absolutely necessary.
- NSM plans should be coordinated with the U.S. Army I3A NSM working group, affected management centers, Major Commands (MACOMs), Directors of Information Management (DOIMs), Commanders-in-Chief (CINCs), U.S. Army units, etc.

6.3 I3A NSM Initiative

The U.S. Army I3A NSM working group is currently in the process of developing the U.S. Army NSM Sustaining Base Architecture in accordance with the new DoD NSM structure under development. While these changes are not complete, it is useful to mention this structure so that U.S. Army organizations are aware of the possible changes that could affect the design of U.S. Army NSM systems. To help ensure that NSM implementations are synchronized across the U.S. Army enterprise, U.S. Army programs fielding networks and/or systems to installations are highly encouraged to coordinate their NSM solutions with the U.S. Army I3A NSM working group, the appropriate TNSOC, and affected DOIMs. This will result in the following benefits:

- Minimize duplication of existing functionality
- Reduce the need for multiple NSM servers at each installation
- Reduce personnel, equipment, and operational costs
- Increase integration

6.4 Network Management Definition and Characteristics

Network management is a set of common activity domains with associated functions and tasks that must be accomplished to establish and maintain a network. Effective and efficient network management maintains the operational status of the network, optimizes its performance, accounts for its usage, and protects the services it provides. Network management essentially is broken down into seven activity domains. Each domain represents a different way of aggregating and distributing management authority and/or management scope for a given activity. Network and information system management resources are partitioned into the domains to make the inherent complexity of NSM manageable. These domains and their associated functional areas are detailed in paragraph 6.7.

6.5 Systems Management Definition and Characteristics

Systems management refers to the monitoring and processing of information and data processing resources, associated peripheral devices, supported applications, and the network communication infrastructure that connects the end users and all components of the system. These systems are usually present at various installations and are often remotely administered from a centralized location. A centralized NSM concept may be appropriate for systems with some or all of the following characteristics:

- Span many U.S. Army or DoD installations
- Have common data sharing
- Have a common architecture
- Require centralized access control
- Require wide area communication between the various elements of the system

6.6 DoD Network Management Control Hierarchy

The Global Information Grid (GIG) supports joint, combined, and service component operations and the strategic, operational, and tactical forces that execute them. C2, intelligence, and mission support are the three disciplines critical to the warfighting forces. The GIG NSM control centers ensure that the warfighter and all DOD components can obtain and sustain responsive, reliable, secure, and effective GIG services. The following paragraphs identify the NSM hierarchy and describe the organizations that manage and control the GIG by performing

NSM activities, functions, and tasks. Detailed information pertaining to these control centers and their functions are found in Chapter 3 of Army Field Manual (FM) 6-02.71.

6.6.1 Defense Information Infrastructure (DII) Operations Control Complex (DOCC)

The DOCC is the functional element through which the DISA Director exercises operational direction and management control of the GIG. The DOCC includes the headquarters DISA staff elements and GIG control centers responsible for managing, controlling, and monitoring the GIG. The primary functions of the DOCC include operational direction over the GIG, operational control of the assets under DISA's purview, and the collection and dissemination of status information.

Note: GIG has replaced DII as the descriptor for the communications infrastructure that supports DoD. However, to date the name of the DOCC has not changed.

6.6.2 Global Network Operations and Security Center (GNOSC)

The GNOSC includes the network management tools, organizations, personnel, and resources to perform NSM activities, functions, and tasks at the global level of the GIG. Located at DISA Headquarters in Arlington, Virginia, the GNOSC provides the overall management, control, and technical direction of the GIG. The GNOSC interfaces directly with RNOSCs, which, in turn, interface with their respective LCCs.

6.6.3 Regional Network Operations and Security Centers (RNOSCs)

The RNOSCs are DISA operated and maintained facilities that execute overall operational direction and control of assigned GIG components within their geographical region. The RNOSC includes the network and system management tools, organizations, personnel, and other resources required to perform the day-to-day network and system management over their portion of the GIG.

6.6.4 Local Control Centers (LCC)

LCCs manage CINC, Service, and Agency-unique GIG networks, systems, applications, and services either deployed or at fixed posts, camps, and stations. Examples of Army LCCs are the ANOSC and TNOSCs.

6.6.4.1 Army NOSC (ANOSC)

The ANOSC provides worldwide operational and technical support to the Army's portion of the GIG across the strategic, operational, and into the tactical levels of war. The ANOSC operational concept is to use advanced NSM technologies to support the warfighter in today's split-base/reach-back environment.

6.6.4.2 Theater NOSC (TNOSC)

The TNOSC provides operational and technical proactive and reactive support to the theater strategic and tactical customers on a 24-hour a day basis. The TNOSC performs the NSM activities, functions, and tasks required to efficiently and effectively manage and control the Army's portion of the forward deployed GIG. The TNOSC manages and controls the theater Army component's long haul communications systems, their portion of the strategic DISN and Defense Message System (DMS), and the tactical networks, when deployed. The TNOSC also provides network support to DOIMs in their area of responsibility.

6.6.4.3 Directorate of Information Management (DOIM)

DOIMs are responsible for the information systems on their installations or within an assigned geographic area. Under MACOM guidelines and procedures, DOIMs plan and budget for the installation, modernization, operation, and retirement of the network and systems on their installation. DOIMs work with external O&M entities to ensure the proper operation of the installation-level component of DOD or Army-level network and systems. DOIMs also perform the following:

- Provide O&M of the common-user information system infrastructure on an installation or in an assigned area.
- Provide on-site support and problem resolution coordination for devices that provide access to Army or DOD-level network and systems.
- Share information concerning installation-level information systems and its supporting environment.
- Implement NSM practices IAW DOD, Army, and MACOM policy and guidance.
- Establish policies and procedures for the AO&M of information systems within the area of responsibility.
- Establish support agreements with the U.S. Army Signal Command.
- Coordinate with TNSOCs and ANSOC concerning all aspects of the Public Access Zone (PAZ) and DeMilitarized Zone (DMZ).
- Provide a customer assistance capability on the installation.

6.6.5 Deployed Joint Communications Control Center (JCCC) and System Control (SYSCON) Centers.

The JCCCs act as RNOSCs for the deployed GIG with the main difference being that RNOSCs receive direction from the GNOSC while the JCCC receives direction from the deployed Joint Task Force (JTF) J6.

6.7 Network Management Activity Domains and Functions

The network includes all hardware and software communication components residing in routing, switching, and transmission system components as well as in the communication related hardware and software components necessary to connect to the network (e.g., communication protocols, hubs, etc). Network and information system management resources are partitioned into the domains to make the inherent complexity of NSM more manageable. The seven activity domains are:

6.7.1 Service Provisioning

This activity domain is performed at all levels of NSM control. It adds, deletes, or changes network and information systems services available to the user. The following functions are associated with service provisioning:

- Service request processing
- Resource assignment
- Configuration change implementation
- Subelement installation
- Service modification verification

- Configure end-user equipment

6.7.2 Planning

This activity domain involves taking user requirements and developing the schedule and resources to meet the users needs. It ensures that changes in requirements for services are collected, analyzed, prioritized, cost assessed, and scheduled for implementation. The ultimate goal of planning is to ensure resources are available to meet current and emerging near-term and long-term requirements, and that proposed implementations conform to short and long-term objectives. The functions below are associated with planning:

- Analysis of user requirements
- Technology assessment
- Architecture definition
- Services planning and programming
- Subsystem definition and funding
- Cost benefit analysis
- Performance objectives establishment
- Contingency and restoration planning
- Capacity planning
- System planning
- Integration planning
- Security planning

6.7.3 Engineering

Within this activity domain, network and information systems resources are tailored to meet user requirements for service. Engineering bases network and systems design requirements on planning direction that relates to capacity allocation and new services that are to be implemented. The engineering activity domain is required from the strategic GIG level of NSM, down to the tactical NSM performed by a NOSC. The following functions are associated with NSM engineering and performed to varying degrees at the different NSM levels:

- Planning assistance to users
- Network and systems design
- Security design
- Facility and equipment design
- Integration of operations, facilities, and equipment
- Technical documentation
- Information systems support and development
- Equipment and services specification
- Implementation design and procedures development
- Technical assistance

- Hardware and software development

6.7.4 Logistics

This activity domain provides for the logistical support of the network and systems. Logistics includes procurement, handling, storage, packaging, distribution, maintenance, and replacement of materiel such as spare/repair parts and consumable items. The functions below are associated with logistics:

- Preventive maintenance
- Corrective maintenance
- Requisition processing
- Equipment inventory management
- Stockage

6.7.5 Administration

This activity domain performs non-engineering and non-realtime functions that are associated with budgeting, training, procurement, staffing, and other business-related functions. The functions listed below are associated with administration activities:

- Policy and procedure development and maintenance
- Training management
- Program and budget management
- Procurement
- Staffing management
- Chargeback
- Directory services and assistance
- Special services

6.7.6 Service Measurement

This activity domain directly interfaces with the use to monitor user satisfaction with the service provided by the network or information systems components. The functions listed below support service measurement:

- User help desk operation
- Customer service monitoring and control
- Performance analysis
- Quality assurance

6.7.7 Specific Management Functional Areas (SMFA)

The SMFA is the core activity domain that provides the monitoring and control associated with keeping the network and systems operating and providing quality service. The SMFA targets network and communications management, rather than systems management. This activity is performed during the operational stages of the network. SMFA consists of the following functions:

a. Fault management provides for detection, isolation, and correction of abnormal network events. Requirements associated with fault management are:

- Provide event correlation, which is the process of narrowing the fault from a mass of problems to a root cause and it's side effects.
- Isolate the fault location from the rest of the network during troubleshooting.
- Lessen the impact to network operations while the fault is being repaired through network reconfiguration.
- Provide for repair or replacement of failed network component(s).

b. Configuration management controls, identifies, collects data from and provides data to network assets to assist in providing continuous operation of interconnected services. Configuration management is also concerned with the initialization and safely shutting down part, or the entire network. Requirements associated with configuration management are:

- Managing baseline configuration
- Maintaining network and systems configuration throughout its lifecycle
- Maintaining asset status
- Updating network and systems configuration
- Notifying configuration manager of changes
- Verifying configuration documentation availability
- Providing for backup of data and system restoration
- Enforcing software licenses and managing updates
- Providing configuration status input to the certification and accreditation plan

c. Accounting management involves gathering data on the utilization of network and system resources and tracking the use of these resources by users or user groups. It provides the ability to bill users, allocate resources based on usage, and plan for future network and system growth. Accounting management may also be useful in the following scenarios:

- A user or group of users may be abusing access privileges and burdening the network at the expense of others.
- Users may be making inefficient use of the network, and the network manager can assist in changing procedures to improve performance.
- The network manager is in a better position to plan for network growth if user activity is sufficiently understood.

d. Performance management provides the capability to evaluate and report on the behavior of managed devices and networks. It allows network and system managers to monitor, analyze, tune, control, and report on the health of network and system components and make changes as necessary. Tasks associated with performance management include:

- Dividing the network or information systems into subnetworks or subsystems and subcomponents and directly sampling and quantifying pertinent metrics.
- Analyzing measured data on an individual subsystem basis and an overall system basis.

- Determining if the network or systems are performing according to technical standards and specifications.
- Analyzing the measured performance data to determine trends, such as increasing or decreasing demands on network or systems resources, and identifying possible problem areas, such as indications of probable subsystem failure or system bottlenecks.
- Reporting general performance problem areas to the network manager.
- Reporting specific performance problems to the trouble desk, to include reporting problems requiring long-term planning or engineering solutions.
- Performing traffic and loading studies.
- Evaluating enhancements.

e. Security management manages the network or information systems security services. Security management controls and monitors mechanisms that exist to protect selected network or information systems resources, user information, or security objects.

Requirements associated with security management include:

- Controlling access to resources, which grants or restricts access to the entire network or information systems or selected critical parts.
- Archiving and retrieving security information which involves gathering, storing, and accessing the information for analysis, detection, and control purposes.
- Managing the encryption process.

Note: Detailed information pertaining to NSM Activity Domains, Functions, and Tasks may be found in Chapter 4 of FM 6-02.71 (11-71).

6.8 Selecting an NSM Solution

Installation level NSM is accomplished by the DOIM. DOIMs have responsibility for the infrastructure assets on their installations or within an assigned geographic area.

There are three scenarios for accomplishing NSM at the installation level:

a. Provided there is WAN connectivity, a small-scale system could elect to be managed by a centralized NSM facility such as the ANOSC.

b. The DOIM would oversee system access to the LAN and WAN, configure and control user access to the system, and manage the system resources (i.e., the software and hardware). Under this scenario system developers should ascertain the answers to the following questions when developing or purchasing an NSM solution:

- What goals and objectives must the system meet?
- How much will the system cost (cost to operate and maintain, cost to design and develop)?
- Will the proposed system integrate into and enhance current IS support capabilities?
- Is the proposed system modular in design?
- Is the product proposed just an element management system or is it an integrator of element management systems?
- What must the system monitor and control?

- Will the proposed system result in more efficient business processes and overall operational savings?

c. The functional system users could manage their own system. This would be a special case where the system has a well-defined local mission that can be managed effectively by the users without extensive interfaces into other systems and, most importantly, the users have the capability to perform the necessary NSM management tasks on their system.

6.8.1 Business Case Requirements

The NSM must solve a business problem or increase efficiency of the current methods of accomplishing work while reducing overall costs. The solution must be economically feasible while providing better service. Developing a set of business case requirements supporting these points will also aid in obtaining management support that is necessary for any significant IS implementation.

Developing a business case requires information gathering. The problem must first be defined in a general sense in order to identify specific network management problems. The first step can be summarized as "understanding what needs to be managed." This step is difficult since many users don't have a clear understanding of detailed management requirements.

The developer of the business case must examine how each section accomplishes day to day activities. The case for network management can be defined by documenting current work processes that may be automated by the system as a whole. Each of the work processes to be automated need to be documented and addressed in the system design and implementation. Of main concern are ways to save the organization money and for ways of making the IS organization, and the services they provide, more efficient (http://netman.cit.buffalo.edu/Doc/DStevenson/ - BCR).

Once developed, these business case requirements will drive the NSM solution since the functions associated with these requirements must be available in order for the users to perform their duties. The business case requirements can be further refined during the engineering process to help ensure that the solution solves a business problem or increases efficiency.

6.8.2 Requirements Definition

Once the basic business case requirements have been established, they can be further refined during the engineering process. Other issues to consider during this step are as follows:

- Identify NSM information exchange requirements for the system being developed. What organizations and/or systems will the NSM system need to interface with and what type of information will need to be exchanged? What are the integration issues associated with these interfaces?
- Investigate ways to improve the processes identified while developing the business case requirements (e.g., automate manual processes, eliminate redundant processes).
- Develop a totally new process from scratch (process re-engineering) with plenty of feedback from the users and system developers (if different from the engineers developing the NSM system). The goal is to eliminate management processes that do not solve real business problems and add only those processes that solve problems and improve efficiency.

6.8.3 Initial Design

The next step is to begin designing the system based on the information collected so far (i.e., business case requirements, requirements definition, technology available, etc.). From this information, choices can begin to be narrowed down and the most promising technologies/products can be identified so that evaluations can be conducted in order to make the final selections. The goal of the initial design should be to map NSM requirements to NSM capabilities. Other initial design considerations include:

6.8.3.1 Network Bandwidth Utilization for NSM

NSM is a support function and as such should not consume a large amount of bandwidth. The goal should be to minimize NSM bandwidth utilization.

6.8.3.2 Backup and Recovery Resource Usage

Backup and recovery communication loading has proven to be the biggest single WAN loading factor associated with NSM on current systems. Backing up large databases can take a large amount of system resources including the communication network and the processors associated with backup and recovery. Backup time can be cut by first compressing the data on the server where the data is located, then backing up the compressed file to the backup system. Another approach is to decentralize storage by putting the storage devices as close as possible to the data being backed up. The scheduling of these backup procedures can still be accomplished from a centralized facility, if desired. With this approach it is important to ensure that Continuity of Operations Plan (COOP) requirement are met. Systems should be designed so that the backup and recovery process is as simple and straightforward as possible. For example, keep the OS, applications, and data on separate drives (when possible) and have "Golden Masters" (i.e., master copies of the standard OS and/or application configuration) available for loading the basic system.

6.8.3.3 Processor Sizing

The processing power needed to perform NSM is largely dependent on the functions the NSM processor is required to perform. It is recommended that the NSM processors be sized with future expandability in mind. It is very likely that future versions of the software will require additional resources in order to perform optimally and several new versions can be expected over the life cycle of the hardware. If multiple NSM applications will be running on a single processor it is highly recommended that the configuration be evaluated in a lab environment to ensure that the selected processor configuration is capable of handling the load.

6.8.3.4 NSM Support Staffing

Staffing for NSM requires the proper personnel (i.e., manpower and personnel integration issues) and associated training. Training is critical for all operations personnel to enable them to effectively manage/monitor the various subsystems (e.g., network devices, servers, backup and recovery equipment, etc.) and operate the various NSM software tools. Highly skilled personnel are required for most NSM operations.

6.8.4 Market Survey

A market survey is performed to determine the most promising COTS products available (COTS software and hardware should be used to the greatest extent possible) to address the identified requirements. The first step in this process is narrowing the field so that more detailed information can be collected for each product. It is not recommended that this survey be done using only information acquired from the vendor's Web-site. This information is normally not detailed enough, is inconsistent from one vendor to another, and is often inaccurate (i.e., may not be updated very often). While the vendor Web-sites provide some good information, other sources should be included in order to get a view of the various products in relation to each other. These include trade journals (many have their own Web-site), industry evaluations, and

U.S. Army or DoD evaluations. There are also services (e.g., Computer Select) available that consolidate this type of information in one place. It is also important to contact each vendor directly once the choices have been narrowed down to a few frontrunners. Ask them specific questions related to the identified requirements (e.g., Do your products support SNMP?). Also try to get feedback from some of their customers on how satisfied they are with sales support, technical support, etc. Contacting their U.S. Army and DoD customers can often provide valuable information.

Note: Appendix A identifies the most commonly used NSMs in DoD.

6.8.5 Lab Evaluations

The market survey and initial design work should identify two or three promising products. If possible, a lab evaluation of these leading products should be conducted to:

- Determine which product is the best match for the identified requirements. All of the top contenders should be able to fulfill the majority of the requirements. Each will have its strengths and weaknesses. Some products perform a wide range of functions but aren't the best solution for any given function. Others excel at one or more functions but don't perform other functions well or at all.
- Determine interoperability with other products and/or systems. Is there a requirement for the NSM system to exchange information internally or with another U.S. Army or DoD system? If yes, make sure that the information can be exchanged without excessive customization of one or both systems. The best way to test these interfaces, prior to purchase, is in the lab.
- Determine whether vendor product claims are accurate. It may not be possible or necessary to verify everything, but evaluating the most critical functionality may prevent some unexpected surprises later. This also includes ensuring that the product implements required standards (e.g., JTA-A mandated SNMP standards).
- Gain hands-on experience. Lab evaluations give the engineers and administrators valuable hands-on experience with the product(s) that will be fielded. Various configurations can be tried in the lab environment to determine the optimal design. It will also give the engineers and administrators a better idea of how easy it will be to setup and configure the hardware and software in the field.

6.8.6 Final Detailed Design.

The information obtained during the previous steps should be integrated into a final design for the NSM solution. The design should specify and document:

- System configuration
- Total cost of ownership information
- Interfaces to network devices (routers, switches), other NSMs, servers, and client systems
- Installation instructions
- Infrastructure upgrades, if any
- Implementation phases

During the final detailed design phase, system documentation should be finalized. This documentation includes:

- System design
- System interfaces

    - Data exchange requirements
    - Testing
- Implementation
    - Security and access policy
    - Configuration management plan
    - Training policy and plans
    - COOP plans
    - Operating procedures

6.9 Implementation

The ideal NSM should be designed and implemented around real work processes. Implementation should focus on the tools that support network personnel.

6.9.1 Implementation Issues

One of the challenges of developing NSM solutions is dealing with a lack of standards for the exchange of information between management software products from different vendors. Since virtually all COTS NSM products use proprietary protocols for exchanging information between their management entities, the options available to the engineer are limited. These options include:

- Government developed interfaces. This involves writing customizations to utilize each vendor's published application programming interface (API) and/or command line interface. The advantage of government developed interfaces is that they can be developed based on the government's unique requirements and are not limited to vendor partnerships. The disadvantages are that these interfaces are expensive, time consuming to develop, and the maintenance burden falls completely on the government. The more individual products that are integrated the more complicated this becomes since the interfaces must be updated every time a new product version is released by a vendor.
- Vendor provided interfaces. This involves purchasing "adapter modules" developed by the vendors through industry partnerships. The advantage of vendor-developed interfaces is the vendor is responsible for maintenance and updates, not the government. The disadvantage is that the government is limited to the interfaces the vendors develop and are constrained by their scheduling of updates to these interfaces.

While there are advantages and disadvantages to each approach it is highly recommended that government developed interfaces and customizations of COTS NSM software be avoided as much as possible. Needlessly customizing software because the government is used to doing business in a particular way should be avoided. In many cases, the required functionality is available in COTS products although the look and feel may be different from traditional methods. The engineer should question whether any customizations are really required since they are costly to maintain. One advantage of engineering a new solution is the opportunity to introduce more efficient and cost effective methods of managing government networks and systems. While government developed interfaces and customizations are sometimes required due to some unique characteristics of the U.S. Army environment, it is usually not the most cost-effective solution.

6.9.2 Reasons Most NSM Implementations Fail

a. Lack of Management Support. It is critical to have full financial support for a successful NSM implementation. An additional critical aspect related to the sponsorship of any project is having the full commitment and support from all the elements involved with the implementation. This must be accomplished and established by management before anything else is done.

b. Unrealistic Estimates. Realistic project requirements of time, money, and personnel are critical. The complexity and cost of NSM implementations can be easily underestimated. Experienced personnel who will help avoid unrealistic expectations must be involved in all phases of the project. This does not refer to money only, but also to the amount of manpower, resources, and time required to implement each functional area.

c. Improper Requirements Definition. Often enterprises are usually unfamiliar with NSM systems and their capabilities. It is important to define the requirements and specify the level of detail necessary within the requirement. The following information should be collected and analyzed prior to defining an NSM architecture:

(1) Quantities, types, geographic distribution, and location of systems to be managed (this includes hardware and software configurations). Once this information is on hand, it must be determined what objects within those devices require management.
(2) Existing NSM related functions and processes must be documented, analyzed, re-engineered if needed, and all applicable functionality integrated into the NSM design. Examples of this include existing help desks, software distribution methods, etc.
(3) Program and user specific requirements should be reviewed for feasibility and characterized as essential or non-essential. "Nice to have" features that require customizations can greatly increase the complexity of the ESM system and its life cycle maintenance cost.

d. Poor Project Management. NSM implementations require skill and experience. Enterprise wide implementations should be directed by experienced personnel knowledgeable in system engineering methods and practices who are familiar with the critical factors required for the successful completion of a technical project. When doing a complex NSM implementation with a team lacking extensive NSM related experience, consider acquiring the services of a consultant with experience building and operating large scale commercial enterprise management systems and help desks.

6.9.3 NSM Implementation Recommendations

To lessen the chance of implementation failure the following is recommended:

a. The project must have one system engineer in charge of all technical aspects of the project. Implementations where different entities have control over separate portions of the project will invariably result in major problems. All contract work should report to the same technical point of contact (TPOC), or at least to TPOCs under direct control of the system engineer (SE) in charge.

b. A subject matter expert (SME) should be assigned at the start of the project to help identify potential pitfalls and avoid major problems. The rationale is to avoid making costly mistakes by having experienced personnel involved in the project from start to finish. The SME should have experience building and operating large scale management systems and help desks.

c. Personnel tasked with administering and maintaining the NSM should be involved in the implementation (or at least the fielding), and become familiar with the design and configuration long before the system goes online. This action will preclude a poor hand-off situation where the customer takes over a new system, and knows nothing about its operation, configuration, and maintenance.

d. Comprehensive and accurate documentation must be delivered with the system. This action goes beyond providing the technical and reference manuals that come with the software and NSM tools purchased. The documentation should describe the system in great detail, i.e., how it was put together, software and hardware components and their function, what customizations were made and how, interfaces and protocols, configuration parameters and the files they are located in, etc.

e. NSM personnel must receive thorough training on the system. The training should be tailored to the NSM applications and environment. The training program should be multifaceted and address training needs in every functional and technical area.

f. During system development business processes should have been translated into system standard operating procedures that will govern each management function to be performed. Testing these standard operating procedures are essential for a successful and efficient NSM implementation.

g. Minimize system customization, "bells and whistles" should be included only after careful consideration of the maintenance overhead they generate, and the complexity that they add.

6.10 Outsourcing Considerations

MACOM, DOIM, and PM information technology management staff face increasing pressures from new technologies and competition for trained resources when planning, developing, and maintaining NSM projects. In response, managers have sought to use both internal and external resources to meet business needs effectively. External vendors have been utilized to meet project demands, but concerns over rising costs and contract effectiveness have impacted the decision-making process. The decision whether to use internal or external resources on an NSM project is determined by a mixture of both hard and soft dollar costs related to the more intangible needs, risks, and benefits. Significant benefits will be realized from prioritization and determination of success criteria, allowing the agency to identify a complete and comparable set of costs and benefits regarding resource choices. Resource limitations, in-house skill sets and knowledge, and expected performance and outcome measures are important factors that must be analyzed in making the outsourcing decision. Establishing and analyzing quantitative and qualitative criteria provides a bottom-line total that indicates which staffing decision is most effective and provides the reasoning used in reaching that decision. Outsourcing can be an efficient and effective alternative to using in-house resources, but a full determination of costs and benefits is required to make that decision. Successful decisions are dependent on having a clear understanding of all the options available. The decision whether to use internal or external resources when implementing an NSM solution must be made by:

- Understanding the needs and constraints of the organization
- Identifying and prioritizing the goals of the project
- Identifying and quantifying the appropriate measures for internal and external operations
- Conducting a cost-benefit analysis of the internal and external alternatives

6.10.1 Identifying Goals and Needs

To make an effective decision, one of the first steps is to identify the needs of the organization and understand why outsourcing may or may not be appropriate. It is critical to have a thorough understanding of the environment to be managed, and all management related processes and functions (in particular those that are to be outsourced).

6.10.2 Reasons to Use External Resources

- To have access to technology, skills, and knowledge not internally available
- To improve business processes and enable organizational change
- To provide needed short-term services without adding to ongoing operational costs
- To focus internal IT resources on core strategic plans and projects

6.10.3 Reasons to Use Internal Resources

- To retain skilled personnel who are able to respond directly to agency needs
- To obtain needed services at lower overall costs
- To take advantage of employees' unique insight into a project or the agency's goals
- To have ownership and control over resource and personnel assets

6.10.4 Cost-Benefit Analysis

Once agency needs and goals have been established, a thorough cost-benefit analysis should be conducted. Organizations must identify all internal and external service costs and benefits to make an effective and reasonable comparison. Quantitative and qualitative measures are essential to determine the full impact of the staffing choice. Prioritizing objectives and identifying measures are essential to project success because they influence the costs and benefits of staffing decisions. The staffing decision is based on the opportunity cost of using internal resources and the identification of agency IT needs and costs, and relies on understanding the complete costs of an outsourcing engagement. Some potential costs are:

6.10.4.1 Costs of Outsourcing

- Contract management costs to the agency
- Effectiveness costs from lack of understanding of project objectives
- Higher project costs as organizations may experience greater overall project costs in order to access necessary skills and expertise that are unavailable internally.
- Higher costs from inadequately defined requirements

6.10.4.2 Costs of Using Internal Resources

- Opportunity costs of staff time
- Ongoing costs for additional employees
- Unpredictable costs as overtime occurs and as employees spend varying amounts of time month-to-month working on the project.
- Effectiveness costs if in-house resources are not sufficient or skilled enough for the project.

The key to a successful staffing decision is the cost-benefit analysis. Having a thorough understanding of in-house operational cost, as well as an understanding of the true, total cost of an outsourcing engagement will enable the agency to make the best decision. Project success derives from the ability to perform the desired NSM services or activities. Identifying the best option for obtaining project success also stems from an understanding of the project processes: is the project to be done better, faster, or cheaper? The staffing decision is based upon the best use of agency resources, according to needs and priorities.

6.10.5 Mitigating Outsourcing Risks

Outsourcing relationships are inherently high risk because each side has a completely different set of goals. The client wants to save money. Normally, the client also wants to find a high productivity partner to decrease its IT backlogs, get rid of its biggest IT headaches, and slim its operation down to its core competency. The supplier wants to make money by growing its business, making high-profit deals, and leveraging its position in the market. When entering into an outsourcing relationship, the client should perform the following risk reduction steps:

- Create a strong internal sourcing group
- Assemble a team that develops and maintains internal metrics
- Benchmark the IT capability to establish a productivity baseline .
- Ask the vendor for productivity benchmarks. If the vendor is reluctant, carefully weigh the risks involved with selecting a vendor with no metrics.
- Get an outside advocate to assist in the contract and initial management stages.
- Determine priorities with regard to schedule, effort, etc.
- Update the baseline periodically to assess whether contract goals are being met for each dimension of priorities. http://cutter.com/consortium/press/000425.html

6.11 Benefits of Pilot Programs and Incremental Fielding

Pilot program should be used to incrementally implement the selected NSM tools beginning with those which have been determined to produce the biggest return on investment. Upon reaching a reasonable level of operational success with the initial tools, the process is repeated until the entire suite of NSM tools has been implemented.

It is important to note that this process is never really complete. The process should continue to refine and improve utilization of these tools. The COTS NSM products currently available on the market are extremely complex so it is important to take this incremental approach whenever possible to help ensure success.

6.12 References

- FM 6-02.71 (11-71), Network Management (NM), Initial Draft, July 2000
- JTA-Army, Version 6.0, 8 May 2000, http://arch-odisc4.army.mil/

Technical Guide for Network and Systems Management, USAISEC, August 2000

7.0 INFORMATION ASSURANCE AND SECURITY

7.1 Purpose

The purpose of this section of the I3A Implementation Guide it to provide guidance for the planning, programming, acquisition, and implementation of Information Assurance (IA) and security1 as an integral component of all Army installation information infrastructures. This document and the I3A IA architecture does not specifically address data security, i.e. the protection of individual user or functional data as it resides on a host/workstation or is being processed by software application programs. It is primarily concerned with insuring that the installation information infrastructure backbone is both secure and highly available.

7.2 Scope

The integration and synchronization of IA architectures and implementations throughout the United States Army and Department of Defense (DOD) is essential to insuring that the critical information they process and transmit is both secure and available to the Warfighter in all operational environments. The information contained in this guide is provided for use by all activities or organizations within the Army that are charged with the development, implementation, or operation of IA components on Army installations.

In today's fast paced IA world it is especially critical that all security designers and implementers keep up to date on all applicable policies and programs before planning specific IA implementations for their infrastructure, system, or network. This will facilitate integration with current systems and will enable the designer to identify programs and standards up front that provide procedural or technical guidance. Planning includes identifying security technologies that best fit your installation requirements.

The IA guidelines contained in this document are based on providing all IA services and activities using TCP/IP based tools. This assumption has been made based on the limited security products currently available for ATM-based networks along with their lack of implementation within the Army's information infrastructure. Since all Army networks at the user level are Ethernet based, the security capabilities native to ATM cannot be used, however this guidance has been constructed in such a manner that its capabilities and functions can be implemented on Army installations with ATM, Gigabit Ethernet, or hybrid backbones.

7.3 Section Organization

This document will discuss established architectural guidelines, identify policies and standards at the DOD level and below, identify doctrinal concepts and policies that effect the design process, and architectural templates and standards for implementation of the I3A.

Unlike other sections of this document that provide detailed installation guidelines, this section will outline the IA concepts and functional capabilities that have been used to form the I3A IA Architecture and provide guidelines for their use. These are the conceptual building blocks that the implementing PM will use in designing the specific security solution for each installation. Specific guidelines on the installation and configuration of IA products is not provided and will be developed as a part of the PM provided security solution. It is further assumed that all hardware and software (HW/SW) will be installed and configured IAW best accepted practices, current DOD, Army, MACOM, and other guidance as may be applicable.

[1] Within the context of this document, the term Information Assurance or IA will include both information assurance and security.

The section begins with an explanation of how the DOD computer network Defense-In-Depth strategy will be implemented on army installations. Defense-In-Depth as envisioned within DOD includes all communications, computer, and network assets that together comprise the Global Information Grid (GIG) down to the end-user workstation. In order to provide the reader with a comprehensive overview, the general IA security planning methodology presented in this section addresses implementing Defense-In-Depth to the end-user level even though the I3A IA Architecture and I3 Modernization Program (I3MP) does not go down to the workstation. The section includes a description of the major functional components and concepts that are currently included in the I3A IA architecture. A description of each building block is provided including high-level diagrams and basic explanations of how they can be used in building security solutions that will increase the overall security posture of the installation backbone. The last part of the section identifies some of the emerging networking and IA technologies and products that will impact Army installations in the near-term.

7.4 General

The installation I3A backbone is responsible for providing a secure networking environment in which systems can safely operate. This includes securing the physical media and interconnecting network devices that route or switch data. The backbone itself does not necessarily provide end system to end system support, since this may include one or more WAN segments, but it is responsible for insuring that data is delivered from one location to another on the installation or to an external network gateway. It must do this in a manner that is timely and provides an acceptable level of protection from unauthorized access and/or manipulation. The infrastructure will employ devices that can enforce DOD, Army, MACOM, and local policies pertaining to acceptable information activities, e.g. services provided and acceptable source/destination addresses.

There is no standard security solution, i.e. specific combination of hardware and software that will be implemented at every installation, however there are standard devices or combinations of devices that will be used to form the specific security solution for each installation. Security designs and implementations for each installation will be based on the solution sets contained in this document and will be tailored to meet the operational requirements of each installation within available resources. In designing security solutions for Army installations, material developers and installation DOIMs alike must adhere to generally accepted systems engineering principles and practices. This will help insure that specific security solutions developed and implemented by individual installations, enclaves, and systems developers are integrated into overall system requirements. Organizations must fully understand the impact of the solution on the system, and the need to insure that the solution is properly implemented. A poorly planned design and/or one that is improperly implemented will likely do more harm to security than good. Therefore, all facets of security planning must be properly integrated and implemented into existing and future systems.

At all times, care must be taken to ensure that physical and electronic access to the infrastructure is limited only to those systems and/or individuals who are authorized access. The physical media must be afforded protection to deny or detect any attempt to gain unauthorized access or any condition that results in a denial of service. Remote management shall only be accomplished if the system can provide for secure Identification & Authentication (I&A) and secure interaction. Across multiple installations care must be taken to insure that allowing electronic access to IA components for the purpose of conducting management and maintenance activities does not increase the threat to the entire installation infrastructure.

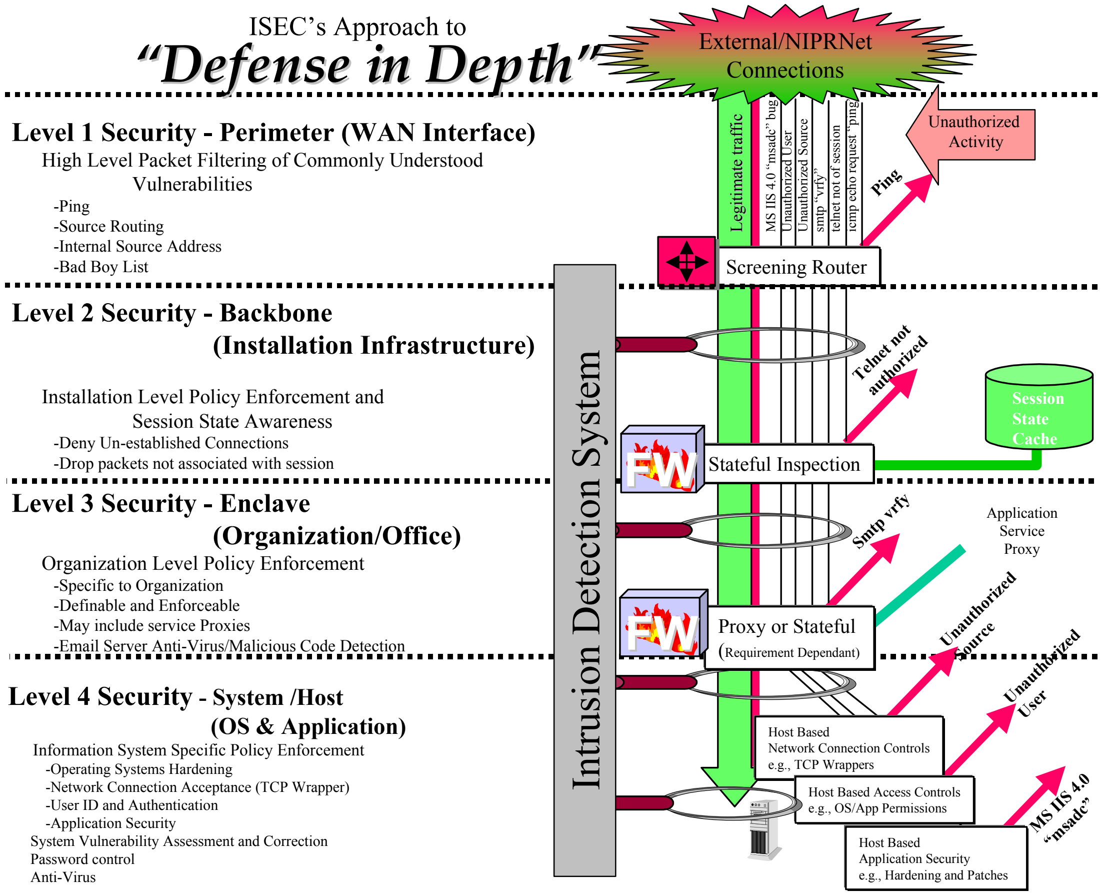
It is incumbent upon the installation backbone to insure timely, secure, and reliable delivery of data. However, it must be recognized that the data that is delivered can only be as reliable as that which is inserted into the backbone and that the reliability of that data is directly related to the security of the end system. End system security is the responsibility of the system developer and the end-user. It is not the responsibility of the installation backbone infrastructure.

The installation DOIM must insure that the networks linked to the End User Building (EUB) Edge Device meet minimum network interface requirements. Service Level Agreements (SLAs) between the DOIM and user activities should be used to define specific host/server configuration and connectivity requirements along with any limitations on the interfaces that the end systems may use or access. SLAs may be used to define the conditions under which a DOIM would be authorized to disconnect or deny service to any organization that fails to adhere to minimum connectivity requirements. Specific DOD minimum IA requirements supporting a Defense-In-Depth approach are being defined as part of the GIG and will be published upon final approval. All networks and end systems connected to the installation backbone shall be installed and configured in accordance with current applicable policies and commonly accepted security practices. Physical and business practice security policies and procedures must be in place and enforced prior to connecting any system to the installation infrastructure. End-user network interface requirements must be coordinated with the end-user/system's network administrator and approved by the installation DOIM to insure that proper access controls are in place and that operational capabilities are maintained without compromising the security of the installation backbone or other users that are connected to it. As a part of the approval process it may be necessary for the DOIM to conduct periodic inspections to verify compliance with connectivity criteria.

7.5 Defense In Depth Methodology

DOD has directed that all Services and agencies adopt a Defense-In-Depth strategy and implementation methodology to protect their computer processing systems and the underlying network infrastructures that connect them together. The Army is implementing Defense-In-Depth through its Network Security Improvement Program (NSIP). Key to defense in depth is the concept of layered security solutions that are implemented to address specific threats or vulnerabilities. The specific solutions are located where they can provide the widest protection with limited interference to functional requirements. To fully protect critical Information Technology (IT) assets on the installation these IA solution sets must extend from the interface between the installation and the Wide Area Network (WAN) down to individual routers, switches, servers, or workstations. Installations will normally be connected to the Defense Information Systems Network (DISN) however installations may be connected to other GIG approved WANs, e.g. Defense Research and Engineering Network (DREN). The I3A IA Architecture is a key element in implementing the NSIP program on Army installations.

Underlying this approach is a multifaceted protection philosophy that is intended to protect the information processing and transport infrastructure from harm while still allowing legitimate, authorized users access to the information and services that the infrastructure was built to provide. It is recognized that protection of the network infrastructure is just as critical as the protection of the individual systems that utilize that infrastructure.


ISEC's Approach to
"Defense in Depth"
External/NIPRNet Connections
Level 1 Security - Perimeter (WAN Interface)
High Level Packet Filtering of Commonly Understood Vulnerabilities
-Ping
-Source Routing
-Internal Source Address
-Bad Boy List
Legitimate traffic
MS IIS 4.0 "msadc" bug
Unauthorized User
Unauthorized Source
smtp "vrfy"
telnet not of session
icmp echo request "ping"
Unauthorized Activity
Ping
Screening Router
Level 2 Security - Backbone
(Installation Infrastructure)
Installation Level Policy Enforcement and Session State Awareness
-Deny Un-established Connections
-Drop packets not associated with session
Telnet not authorized
Session State Cache
FW
Stateful Inspection
Intrusion Detection System
Level 3 Security - Enclave
(Organization/Office)
Organization Level Policy Enforcement
-Specific to Organization
-Definable and Enforceable
-May include service Proxies
-Email Server Anti-Virus/Malicious Code Detection
Smtp vrfy
Application Service Proxy
FW
Proxy or Stateful
(Requirement Dependant)
Unauthorized Source
Unauthorized User
Level 4 Security - System /Host
(OS & Application)
Information System Specific Policy Enforcement
-Operating Systems Hardening
-Network Connection Acceptance (TCP Wrapper)
-User ID and Authentication
-Application Security
System Vulnerability Assessment and Correction
Password control
Anti-Virus
Host Based Network Connection Controls e.g., TCP Wrappers
Host Based Access Controls e.g., OS/App Permissions
Host Based Application Security e.g., Hardening and Patches
MS IIS 4.0 "msadc"

At each level within the architecture, care must be taken to examine the potential threats and vulnerabilities and assess the risks posed to critical IT assets. With this information, it then becomes possible to form a plan for implementing protective measures that will eliminate or mitigate the identified threats or vulnerabilities to the maximum extent possible within available resources. For example, it is incumbent upon the network infrastructure to halt all traffic that is obviously of malicious intent. Care must be taken to block this kind of activity at all levels. There are some specific commands and actions that only have the purpose of causing denial of service to the installation network or a host/server therein. These commonly understood malicious activities are blocked at the installation boundary by Army policy. In general TCP/IP services, ports, and protocols that are not specifically required should be disabled. However, care must be exercised to insure that this does not adversely impact mission accomplishment. Measures must also be taken to protect the infrastructure from infection by viruses and other forms of malicious independent code.

Figure 7.1 Defense-In-Depth

As illustrated in Figure 7.1, four basic levels must be addressed in order to provide comprehensive protection for critical IT assets. Such a layered approach helps to ensure that maximum interoperability is maintained and that the degree of security matches the specific requirements and capability of the security solution owner to implement at each level. The right side of the diagram depicts a data flow along with six threads that either violate a sample security policy or are commonly encountered attack mechanisms. The left side provides descriptions of the types of security policies that should be encountered at each level while the center shows sample security tools as well as suggested locations for countering the specific example attack threads shown.

The basic protection philosophy employed in the Army's Defense-In-Depth approach is that security restrictions become less restrictive in nature as one moves from the end-user/server enclave environment through the installation backbone to an external network interface. In other words, the most restrictive controls and mechanisms will be implemented closest to the data or component that they are intended to protect. This philosophy ensures that security is implemented in a manageable process whereby system specific policies are enforced closer to the system, where the likelihood of full understanding of the system's requirements is greater. At the WAN interface this means that security provisions will generally be minimal, basically just blocking protocols and addresses that are universally unacceptable across all installations. As you enter the installation backbone from an external network gateway or interface you can then begin to implement installation level security policies. The types of policies enforced at this level will be more installation specific and restrictive than those implemented at the WAN interface, but still of a more general nature than enclave or system level policies. Implementing policies at this level provides that ability to provide a good minimum level of assurance without having to be intimately familiar with the specific ports, protocols, and processes used by each end system. As you enter the enclave level you have finally reached a level where an organization or system administrator should be able to understand specific system network interface requirements, i.e. port, protocol, and processes, and system vulnerabilities. This is also the appropriate level for very specific security policies and protective mechanisms to be implemented and enforced. It must be clearly recognized that regardless of the type and number of network based security solutions implemented, there will always remain security concerns and vulnerabilities that can only be mitigated at the host/server level.

These basic protection principles must be applied at all levels of the installation's logical IT architecture. For instance, at the installation WAN gateway a mixture of all four levels should be encountered while within an organization's LAN one might only find implementations of Levels 3 and 4. It is important that IA/security implementations across an installation are coordinated and comply with all higher level policies, guidance, and standards. Organizations must adopt and implement commonly accepted best security practices and all IT components will be installed and configured to protect them from any commonly known vulnerabilities associated with them to include the implementation of all applicable Information Assurance Vulnerability Alerts (IAVA).

The I3A IA architecture and I3MP currently addresses Levels 1, 2, and portions of Level 3. It provides broad guidance for implementing three basic security/IA solution sets including a common installation Top Level Architecture (TLA), a variety of computer network defense demilitarized zones (DMZs), and protected server farms. The descriptions in this document of the various levels and their components will be focused on the functional capabilities that are provided. Specific product recommendations or descriptions are only provided where specific decisions that affect a large portion of the Army community have been implemented. Layer 3 is jointly the responsibility of the DOIM and the enclave owner. Organizations that own enclaves must coordinate IA measures with enclave tenants to ensure that system connectivity is maintained. Level 4 security at the system host/workstation level is the responsibility of the individual organizations and users. As already has been stated functional data owners are responsible for the security and protection of the actual data as it resides on or is processed by software applications.

7.6 Top Level Architecture

The Top Level Architecture (TLA) addresses the IA measures that will be employed at the network boundary between the installation I3A backbone or Installation Campus Area Network (ICAN) and all external network connections. Examples include but are not limited to the DISN Wide Area Network (WAN), the Defense Research and Engineering Network (DREN), and direct connections to other sites and organizations e.g. support contractors. The TLA provides Army installations with a security hardened defensive perimeter that can be used to enforce Army wide policies and provide and maintain a minimum, Army-wide security posture and architecture.

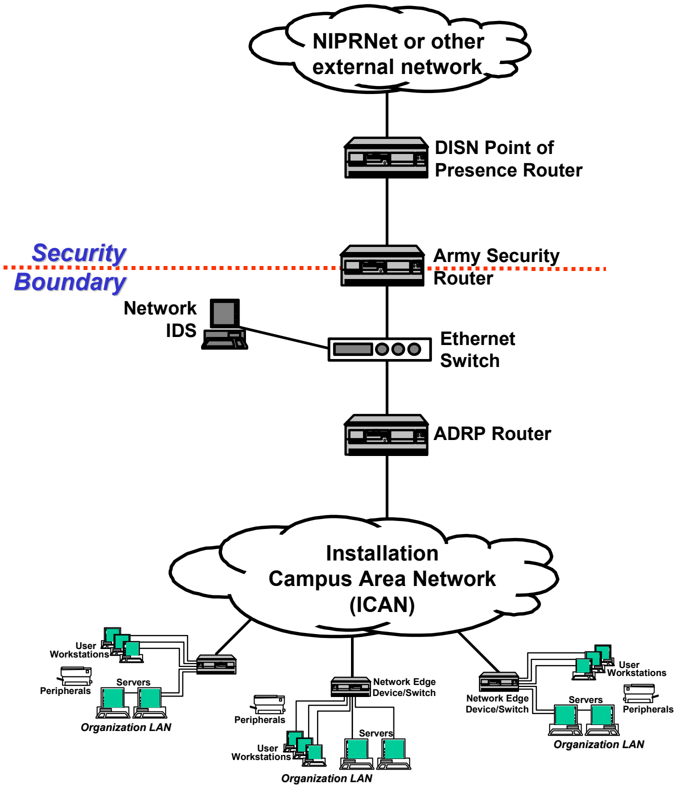


Figure 7.2. Top Level Architecture (TLA)

The functions of the TLA are currently provided by the Army's NSIP Security Stack that consists of a security screening router, Ethernet Switch, and network intrusion detection system (IDS) as shown in Figure 7.2. The TLA/NSIP Security Stack will generally be located in the same facility as an I3A Main Communications Node (MCN). Like MCNs, the specific number of TLA/NSIP Stacks at an installation will be based on its size and communications requirements. The functional configuration of the TLA has been standardized across the Army and installed at over 150 locations. Originally the types of components within the TLA were also standardized however as installation specific requirements have changed over time the current TLA components may vary in size, processing power, and performance characteristics. Any new circuit or connection between an Army installation backbone network and any external network must be routed through a TLA configuration. An existing TLA configuration may be used if the requirement(s) for the new connection do not exceed its capacity. If the new connection exceeds the port capacity or performance characteristics of the existing TLA, an additional TLA configuration may be required to support the new connection

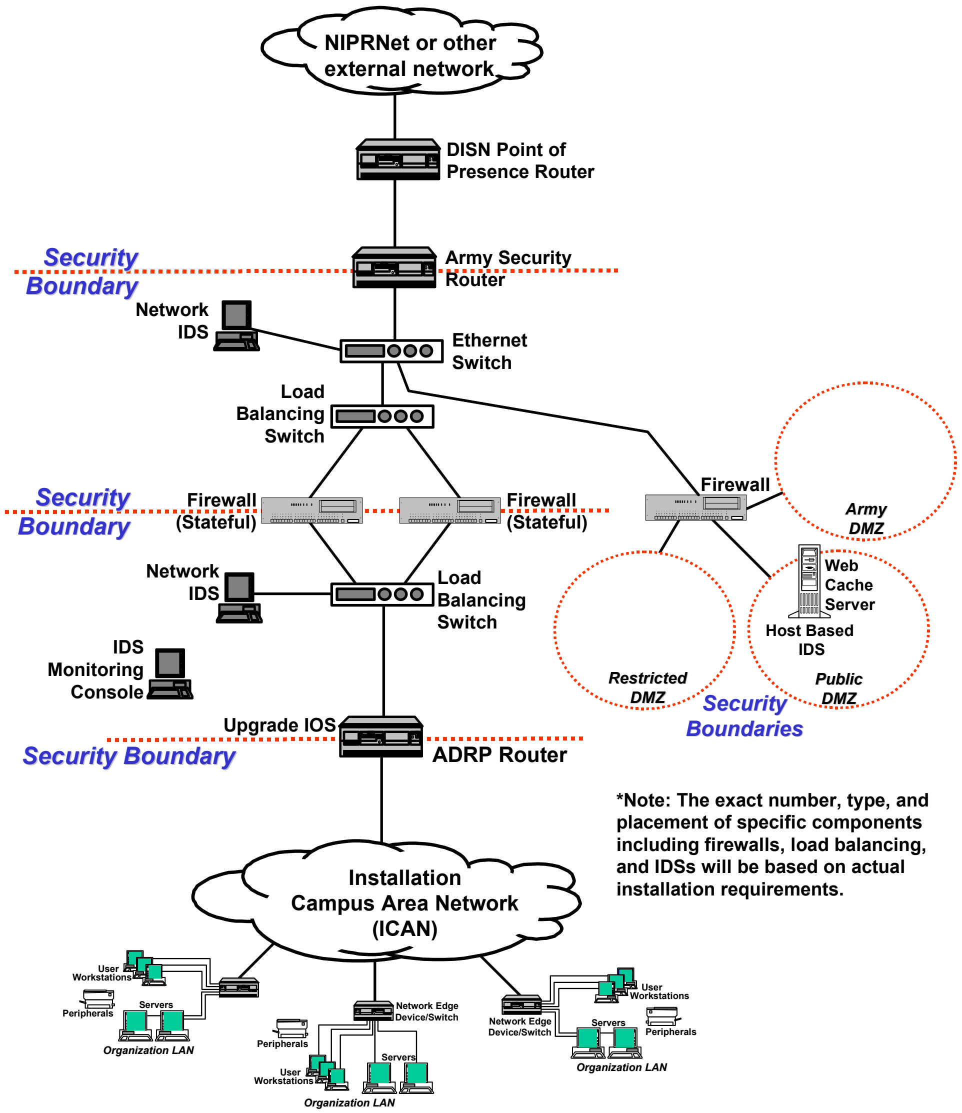
In addition to its routing functions, the security screening router provides the Army with the operational capability to quickly implement Access Control Lists (ACLs) that can be used to block specific IP addresses, ranges of addresses, and/or ports, services, or protocols as may be required. Those addresses that are blocked are ones that are either known or suspected of having been used as avenues for probes or attacks directed against commercial, government, or some portion of the DOD or Army network infrastructure. The security router is also used to block or filter specific ports, protocols and services that are deemed unnecessary for entry onto an Army installation, e.g., unauthorized (Simple Network Management Protocol (SNMP) requests. Controlling access through the use of ACLs is an important and fundamental IA technique and one that will be frequently encountered.

The associated Ethernet switch and network IDS provide a near real-time monitoring capability that enables the Army to quickly identify and react to a large number of common types of network attacks and other hacker/malicious activity that might be directed against its networks, systems, and users. All TLA Army level IDS engines are centrally monitored by one of the Theater Network and Systems Operations Centers (TNSOC). Currently the Army Signal Command (ASC) operates the CONUS TNSOC[2] at Ft Huachuca, AZ, the European TNSOC in Mannheim, FRG, the Pacific TNSOC at Ft Shafter, HI, and the Korean TNSOC at Camp Walker, ROK.

The final component and second layer of security in the current version of the TLA is the ACL capability provided by the Army DISN Router Program (ADRP) router. Unlike the TLA security router ACL, the ADRP ACL is managed and controlled by the local DOIM. As part of the overall network security planning process, the local DOIM may find it useful to implement additional installation specific access controls that further limit access to the installation backbone. When general access controls beyond those implemented at the TLA security router are implemented at the ADRP router, care must be taken to insure that service to customers and systems connected to the installation I3A backbone are not disrupted.

Initially implemented in 1998 as a “hasty network defense” the TLA by itself is not adequate to meet the growing performance and security requirements of Army networks. In recognition of this, efforts are currently underway to enhance the current TLA design and implementation. Figure 7.3 depicts a notional enhanced TLA objective architecture that might be found at a large installation.

[2] More commonly known as the Army Network and Systems Operations Center (ANSOC).



*Note: The exact number, type, and placement of specific components including firewalls, load balancing, and IDSs will be based on actual installation requirements.

Figure 7.3. Enhanced Top Level Architecture (Notional for Large Installation)

7.7 Computer Network Defense Demilitarized Zones (DMZs)

Computer network defense demilitarized zones or DMZs are used to create one or more electronic information areas within a network where IT assets can be physically or logically separated from the majority of a network, e.g. from the post, camp, or installation I3A backbone. The primary purpose of the DMZ is to provide a means of defining and enforcing one or more security or access policies for systems that are primarily accessed by users that are external to an installation or organization or whose primary interface is with an external network, e.g. DISN.

DMZs may be created within a computer network in different ways and using different types of equipment. One way as shown in Figure 7.4 is to establish two or more perimeters or protective layers using devices that can implement an ACL or other restrictive mechanism. The outer perimeter is then configured to allow access to any user. Succeeding perimeters are configured with access controls that are each more restrictive than the proceeding one. This allows for the creation and enforcement of two distinct security or access policies, with the inner one being more restrictive than the outer one. In all cases access should be denied to those IP addresses associated with malicious activity or those that have been approved for blocking by the appropriate authority.

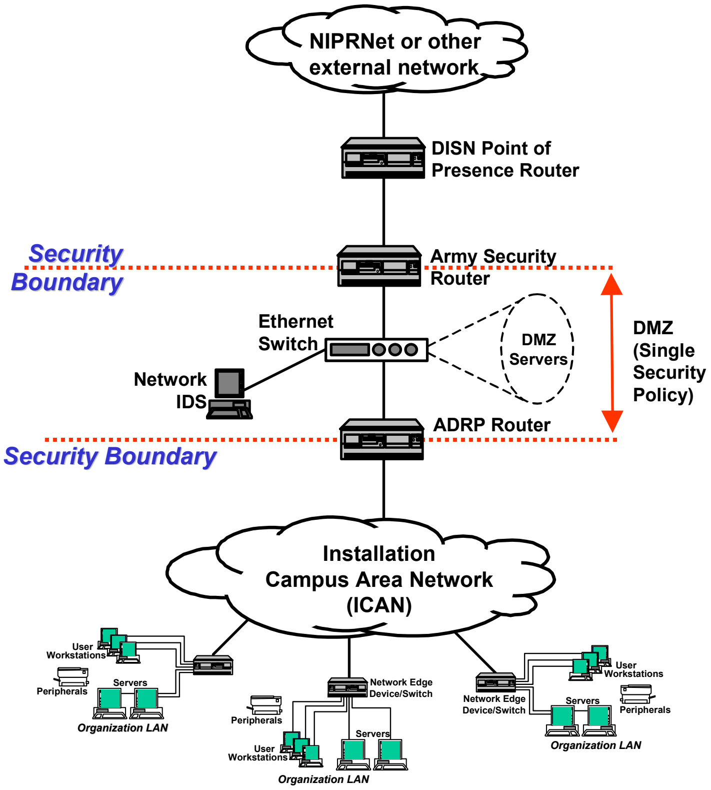


Figure 7.4. Single-Zone DMZ

Although this type of DMZ implementation can be used to provide standard levels of protection to all of the assets in a security layer, it does not provide a great deal of flexibility in its implementation since a single policy governs access to an entire layer. This type of DMZ implementation normally requires separate security devices at each layer to act as boundary control devices. Therefore, each additional layer of protection adds another device increasing overall system requirements, e.g. systems administration, configuration, and maintenance. It also increases the complexity of troubleshooting and network management.

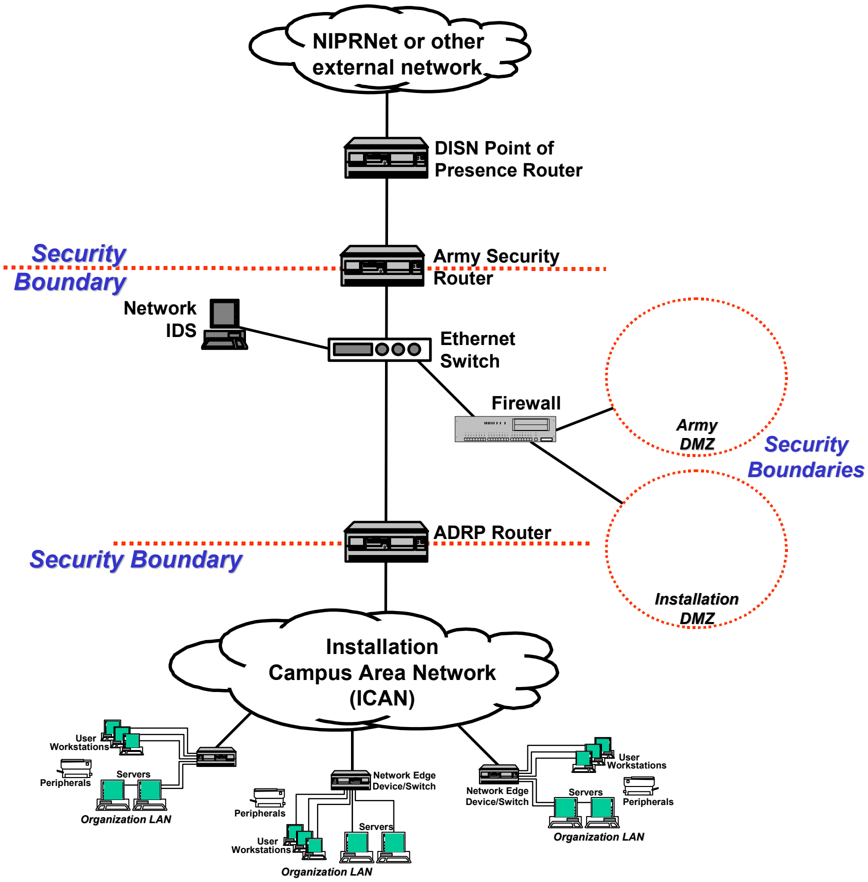


Figure 7.5. Multi-Zone DMZ (Example #1)

A much better approach for implementing an installation DMZ is shown in Figures 7.5 and 7.6. Here, a DMZ breakout device such as a firewall equipped with multiple ports that can each enforce a different security policy is used. In this way, three or four different security policies can be implemented and enforced depending on the specific capabilities of the breakout device that is used. This type of DMZ can significantly reduce the systems administration and configuration overhead costs per security policy since they only require a single device to maintain multiple policies.

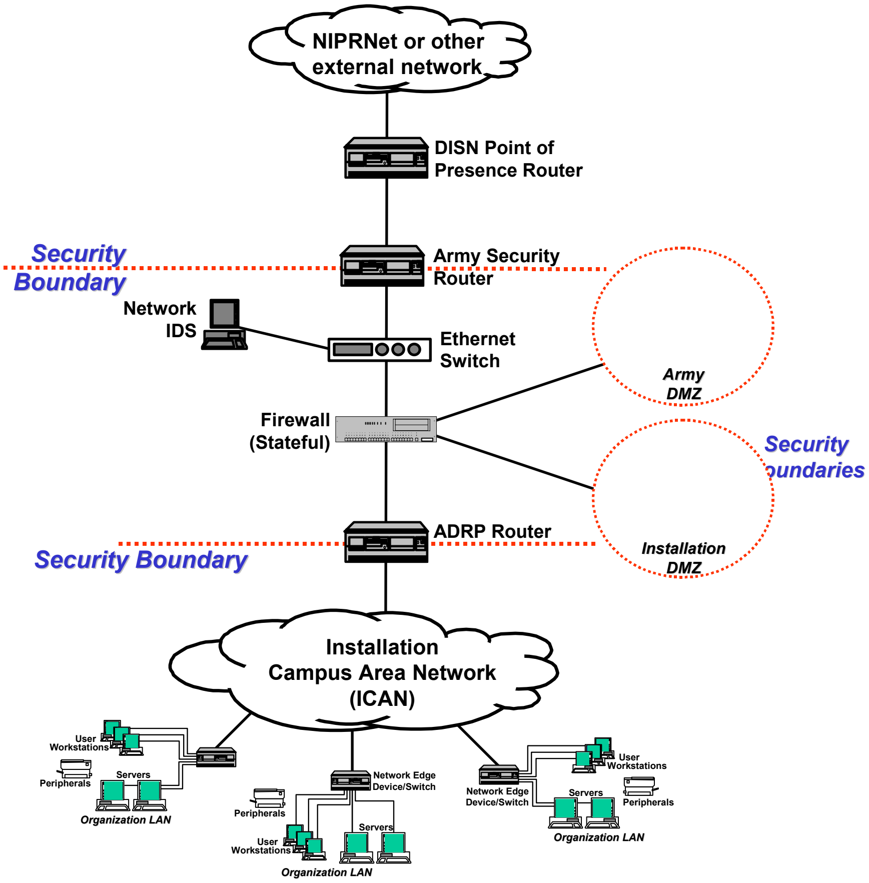


Figure 7.6. Multi-Zone DMZ (Example #2)

DISC4 guidance calls for establishing an Army DMZ that will contain designated critical IT assets under central configuration management control and monitoring.[3] The Army DMZ is currently located in the TLA between the security and ADRP routers as shown in Figure 7.4. The common access nature of the servers placed in the Army DMZ makes it especially important that they be security hardened and equipped with additional IA products as may be required. Specific recommendations for protecting critical servers placed in the Army DMZ will be made by the system developer and will be approved by DISC4 prior to implementation.

The local DOIM or organization may create additional DMZs to meet installation or enclave specific security requirements for systems that support remote access or require additional protection. Current Army guidance does not specify the type or number of DMZs that an installation may implement. It does however identify two categories of systems that should be placed in a DMZ. First are those servers that have a primary interface responsibility for systems external to the installation and allow public access. Second are those that have primary interface requirements for systems external to the installation, but have definable non-public user and protocol requirements. In the first situation the DMZ security protections will limit protocol and

[3] Note: The most current DISC4 IA policy messages can be found on the Army's Information Assurance website at https://akocomm.us.army.mil/c2p/default.htm. Access to this site requires that users first establish an account with Army Knowledge Online.

service access, but not individual users. In the second case, both user and protocol/service access will be controlled. In every case, only those ports and protocols that are required for the operation of the servers and applications within a DMZ should be allowed to pass through the firewall. Access controls must also be put in place to ensure that only legitimate, authorized users are able to access the information contained within the DMZ.

Each installation DOIM must work with the organizations on that installation to identify the specific types and numbers of servers or other critical assets that will be included in any DMZ. Efforts should be made to reduce the total number of servers that are placed in a DMZ by co-hosting multiple applications/services on a smaller number of servers. For example instead of placing multiple organizational webservers in a public DMZ, implement a single installation public webserver that meets the total installation requirement. After determining what systems, applications, services, etc. will be placed in the installation DMZ(s), it becomes possible to develop an appropriate set of security policies and plan the implementation of IA measures that will protect the DMZ.

Given the performance characteristics of some security products care must also be taken to ensure that their placement does not adversely affect network or system performance. Organizations and activities located behind such a security device must be provided network connectivity and performance adequate to meet their requirements. Configuration of security components on the installation backbone is of particular concern since, if a firewall is not configured correctly, it can bring all network communications to a halt. As a result, security device configurations must be carefully coordinated by all organizations on an installation.

The nature of the Internet communications protocols that networks depend on means that it is no longer possible for individual organizations or installations to have exclusive control of installation security configurations. In order to maintain interoperability across DOD's worldwide networks, and systems all organizations will have to comply with security policies, guidelines, and standard configurations. It will no longer be possible for organizations and activities to implement IA configurations that are arbitrarily more restrictive in nature because doing so could adversely affect a communications or information system that traverses their portion of the network infrastructure. At the direction of the Military Communications Electronics Board (MCEB) and with the full support of the Army Chief Information Officer (CIO), DISA is establishing a central DOD repository that system administrators will be able to access to obtain the TCP/IP protocol, port, and service requirements for DOD systems.

The Army's I3A Information Assurance Working Group (IAWG) is currently developing an Army Protocol Registration Process. Under this process, Army IT system developers would be required to identify and document their specific network port and protocol requirements to a central Army Point Of Contact (POC). After evaluating the operational impacts and security risks associated with each requested use of ports and protocols, a decision will be made on whether or not to approve the use of the requested ports and protocols across Army networks. The Army Protocol Registration Process will also be used to elevate Army requirements to the Joint level so that they can be incorporated into the central repository. Specific information about this process and timelines for its implementation will be published separately upon final approval.

7.8 Protected Server Farms

The concept of a protected server farm or server hosting service allows an installation or organization to consolidate servers that provide critical IT services commonly accessible to an installation at large or to a larger community of users within an installation or functional area. Some types of servers that may be encountered in a server farm include E-mail servers, Intranet web servers, shared file or print servers, and Tier 3 Domain Name Servers under the control of the installation DOIM or tenant organization.

Consolidating a large number of servers in a central location allows an installation or organization to concentrate its resources, i.e. personnel and dollars and provide better protection to these critical assets than if the same number of servers were located in several different areas or buildings. Given that functional servers are normally widely dispersed across an installation, multiple instantiations of protective mechanisms would have to be employed just to provide an adequate level protection for each individual server wherever it might be located. This inherently increases the cost of protecting a large number of servers because it requires the purchase, installation, operation, and maintenance of multiple sets of protective mechanisms. It will also require more people because each functional area will have to have their own personnel to perform systems administration functions for their individual servers. Consolidating servers allows for a smaller number of people to provide a standard level of system administration services and information assurance services to larger number of devices.

Consolidated server farms can also be used to provide controlled access areas where functional servers can be consolidated. In this way, a single set of protective mechanisms can provide a standard level of protection for a larger number of servers. However, consolidating critical servers in a single location can serve to create a new and much more desirable target so the benefits gained from server consolidations must always be balanced against any potential increased risk and extra care must be taken to ensure that adequate protective measures are employed. These might include Wrapper type products, various restrictive access control mechanisms, hardened operating systems, etc. as required that are applied on all servers to meet the specific security requirements of a particular server co-location site.

The specific servers to be included in such farms along with the specific information assurance measures to be used is left up to the discretion of the DOIM and organization that controls the server farm. Typical protective measures could include use of firewall, proxy servers, locally monitored host-based intrusion detection systems, Virtual Private Networks (VPNs), and other IA components that will provide adequate access controls for the IT assets in the server farm.

The DOIM or other organization operating the server farm would typically be responsible for providing a common level of physical and logical IA protection to all of the servers in the server farm along with providing host operating system administration functions and hardware maintenance. The specific services that would be provided should be incorporated into Service Level Agreements between the DOIM as the service provider and users. In most cases the content or actual material placed on the server will not be controlled by the DOIM but rather by the functional proponent, e.g. the personnel system, logistics system, or maintenance system who would retain responsibility for their application software and control the data on their servers.

7.9 Physical Security

In addition to the electronic and protocol aspects of information assurance the issue of physical security becomes critical in a fixed infrastructure. As has been documented in the early sections of this architecture the cable plant and associated equipment, e.g., manholes, ducts, distribution centers and Telecommunications Rooms, all become single points of failure for buildings, organizations, or the entire installation. Very close attention must be paid to physically securing these locations from ground attack, acts of God, or unauthorized activity.

Typically Telecommunications Rooms and distribution centers are contained in reasonably secure facilities. However, the campus cable run is typically left unprotected as it runs across the installation. A single malicious individual, or a coordinated assault on the ducts and manholes housing the installed cable can quickly disrupt or destroy the transport capability. As a prelude to specific or general hostilities this would be devastating on the installation's ability to respond to a crisis. Therefore, a great deal of attention shall be provided to insure that the appropriate physical security specialists have analyzed the various facilities and cable routing and applied appropriate physical security.

The specific physical layout of the wiring and distribution capability needs to clearly indicate the location of the support mechanisms for high profile organizations. Further analysis shall be given to identifying those locations that become high risk due to the exposed nature of the ductwork or manholes, or where the cabling becomes concentrated and a single act could cause greater damage.

7.10 Wireless Connection Security

As addressed in paragraph 5.10 Wireless Connections are becoming somewhat common on Army installations. Use of wireless technologies must be carefully reviewed to insure that backbone connectivity requirements cannot be met using other technical solutions. Wireless LANs and other wireless connection technologies also require specific attention with respect to various areas of information assurance. Most of today's data used by the Army has been deemed to be Sensitive But Unclassified (SBU). All SBU data transmitted via wireless media, in accordance with AR 380-19, must be encrypted. Care must be taken to select a solution that satisfies AR 380-19 encryption requirements or appropriate Risk Management Reviews and waivers must be obtained.

In addition to the privacy afforded by encryption, additional consideration must be given to OPSEC and criticality of service availability. An analysis shall include considering whether or not the intended environment, e.g., retail or wholesale logistics points, can be used as an indicator of military preparedness. Even with encryption the level of data transmission might indicate a heightened state of activity that could be used, along with other indicators, to confirm a specific readiness activity. Additionally, analysis must be given to determine if the function being accommodated by Wireless Connections is critical to the operational mission of the organization. If it is critical, then care must be taken to insure that simple jamming activities cannot be used to create a denial of service. Solutions may include the use of spread spectrum technologies, frequency hopping, or a good Continuity of Operations Plan (COOP) that can easily be implemented without significant loss of function.

7.11 Emerging IA Technologies

Information Assurance is a challenging and rapidly changing environment where new technologies seem to appear almost daily. The I3A Information Assurance Working Group (IAWG) is actively involved in investigating new IA concepts and technologies to identify candidate solutions for use on Army installations. The IAWG gives Major Army Commands and material system developers a forum whereby common requirements can be explored and potential common solutions agreed upon. This centralized, partnering approach will reduce redundancy within the Army and help to limit integration and interoperability issues that could arise if individual systems, enclaves, and installations each were to choose their own unique IA solutions. Defense-In-Depth will be enhanced through the IAWG as common solutions are placed in the architecture and services defined for use across each installation.

The following list represents some of the concepts and technologies that the group is currently looking into and although representative in nature is not intended to be an all inclusive or comprehensive list of everything that is currently available in the commercial marketplace. It should also be noted that many of these technologies are currently being used in different places within DOD and the Army.

- Global Information Grid (GIG)
- Virtual Private Networks (VPN)
- Web Caching
- Proxy Servers
- Scanning E-Mail Servers
- Secure Electronic Commerce
- Public Key Infrastructure (PKI)

As these technologies are integrated into the I3A IA Architecture, separate sections will be for each and incorporated into this document.

GLOSSARY. ACRONYMS AND ABBREVIATIONS

AC	alternating current
ADN	Area Distribution Node
ADRP	Army DISN Router Program
ADSL	Asymmetric Digital Subscriber Line
AFH	Army Family Housing
AIS	Automated Information System
A-MCN	Alternate Main Communications Node
ATM	Asynchronous Transfer Mode
AWG	American Wire Gauge
BISDN	Broadband Integrated Services Digital Network
BTU	British Thermal Unit
C^3I	Command, Control, Communications, and Intelligence
CAN	campus area networks
CAS	Central Authentication Server
Cat 3	Category 3
Cat 5e	Enhanced Category 5
Cat 6	Category 6
CATV	cable television
CC	center-to-center
CCTV	closed circuit television
CEGB	cable entrance ground bar
CMIP	Common Management Information Protocol
CONUS	Continental United States
COOP	Continuity of Operations Plan
COT	central office terminal
COTS	commercial-off-the-shelf
CP	Consolidation Point
CP	center-to-point
CSU	Channel Service Unit
CUITN	Common User Installation Transport Network
DA	Department of the Army
dB	decibel
DC	direct current
DCO	Dial Central Office

DDN	Defense Data Network
DISA	Defense Information System Agency
DISN	Defense Information Systems Network
DNS	Domain Name Service
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instructions
DOIM	Director of Information Management
DPW	Department of Public Works
DSN	Defense Switched Network
DSSMP	Digital Switched Systems Modernization Program
DSU	Digital Service Unit
EIA	Electronics Industry Association
EMT	electrical metallic tubing
ESM	Enterprise Systems Management
EUB	end user building
FDDI	Fiber Distributed Data Interface
ft	foot
GbE	Gigabit Ethernet
GSP	galvanized steel pipe
HQDA	Headquarters, Department of the Army
HVAC	heating, ventilation, and air-conditioning
I&A	identification and authentication
I/O	input/output
I3A	Installation Information Infrastructure Architecture
I3AIP	Installation Information Transfer System Improvement Program
ICEA	Insulated Cable Engineers Association
IEEE	Institute of Electrical and Electronics Engineers
IMA	Information Mission Area
in	inch
IS	Information System
ISDN	Integrated Services Digital Network
JIEO	Joint Interoperability and Engineering Organization
JTA	Joint Technical Architecture
JTA-A	Joint Technical Architecture-Army
kb/s	kilobits per second

LAN	local area network
LANE	LAN Emulation
MACOM	Major Command
MAN	metropolitan area network
Mb/s	megabits per second
MCA	Military Construction-Army
MCN	Main Communications Node
MDF	main distribution frame
MER	Minimum Essential Requirements
MGB	master ground bar
MIB	Management Information Base
MLPP	multi-level precedence and pre-emption
MPOA	Multi-Protocol Over ATM
MS NT	Microsoft New Technology
MUTOA	Multi-User Telecommunication Outlet Assembly
NEC	National Electrical Code
NIC	network interface card
NIPRNET	Non-classified Internet Protocol Router Network
N-ISDN	Narrowband-Integrated Services Digital Network
nm	nanometers
NSM	Network and Systems Management
O&M	operation and maintenance
OCONUS	Outside Continental United States
OPSEC	Operations Security
OSCAR II	Outside Cable Rehabilitation-II
OSI	Open System Interconnection
OSP	outside plant
OSPF	Open Shortest Path First
PBX	private branch exchange
PC	personal computer
PDS	Premises Distribution System
PET	protected entrance terminal
PICS	Protocol Implementation Conformance Statement
PKI	Public Key Infrastructure
POTS	Plain Old Telephone Service
PP	point-to-point

PVC	polyvinyl chloride
REA	Rural Electrification Administration
RF	radio frequency
RMON	Remote Monitoring
RSU	Remote Switching Unit
RT	remote terminal
RUS	Rural Utilities Service
SBU	Sensitive, But Unclassified
SDCO	Small Dial Central Office
SF	square feet
SLC	subscriber loop carrier
SMOC	Security Management Operations Center
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
TC	Telecommunications Closet
TCP/IP	Transmission Control Protocol/Internet Protocol
TIA	Telecommunications Industry Association
TMN	Telecommunications Management Network
TNSOC	Theater Network and Systems Operations Center
TR	Telecommunications Room
UL	Underwriters Laboratory
USAISEC	United States Army Information Systems Engineering Command
USASC	United States Army Signal Command
UTP	unshielded twisted pair
VLAN	virtual LAN
WAN	wide area network
WG	Working Group
WWW	World Wide Web

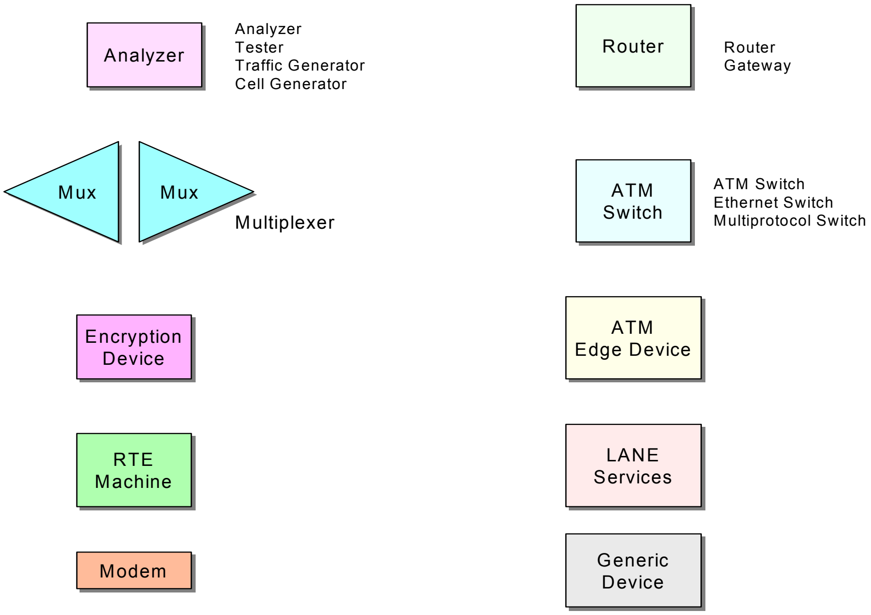
NODES

Main Communications Node

Area Distribution Node

End User Building

Generic Comm Devices



Analyzer

Analyzer
Tester
Traffic Generator
Cell Generator

Router

Router
Gateway

Mux

Mux

Multiplexer

ATM Switch

ATM Switch
Ethernet Switch
Multiprotocol Switch

Encryption Device

ATM Edge Device

RTE Machine

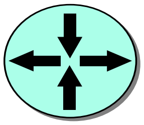
LANE Services

Modem

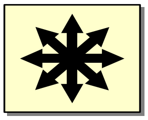
Generic Device

revision

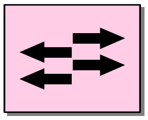
Communication Device Symbols



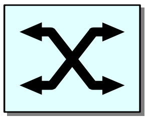
Multi-protocol Router



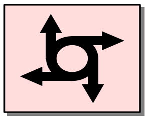
Multi-layer Switch



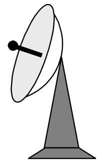
LAN Switch



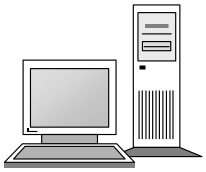
ATM Switch



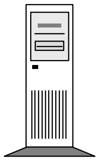
Access Server



Satellite, Wireless



Workstation, Server, Network Mgmt Station



Mail Host or Server